Tactical Communications for the Prepared Citizen

Operating in Remote, Isolated, & Non-Permissive Environments

Michael Chesbro
KD7KLA / WQZH909

Contents

Tactical Communications for Isolated Personnel	2
PACE Communications Planning	3
GOTWA Contingency Planning	5
Dead Man's Switch	5
DoD Communications Planning for Isolated Personnel	7
Radio Watch / Net Control Stations	14
Personal Radio Services	15
Sample EPA Format	17
Wilderness Protocol	21
Repeaters	22
Winlink Global Radio E-mail	26
Emergency Frequencies	27
Satellite Communications	28
Isolated Personnel (IP) with Communication Equipment	29
Near Vertical Incidence Skywave (NVIS)	30
Weather Radio Broadcasts	32
Android Team Awareness Kit (ATAK)	33
Mesh Networks	34
SARDOT & SARNEG	35
DRYAD Numeral Cipher/Authentication System	37
Sample Brevity Matrix	39
Encryption & Field Ciphers	41
Signature Management	43
Calling 911	48
Text to 911	50
Military Manuals and Communications References	51
NATO Phonetic Alphabet, Codes & Signals	52

Tactical Communications for Isolated Personnel

32 CFR § 158.3 defines **Isolated Personnel** as *"U.S. military, DoD civilians, and contractor personnel (and others designated by the President or Secretary of Defense) who are unaccounted for as an individual or a group while supporting an applicable operation and are, or may be, in a situation where they must survive, evade, resist, or escape."*

Field operations today require individuals to work in smaller, more agile teams across widely distributed geographic areas, in often remote, austere, and wilderness environments. Personnel in these areas frequently cannot maintain line-of-sight communications with a headquarters or basecamp, let alone with others operating in the area - even when these other teams are just a few miles away.

Outside of the military environment we may define isolated personnel as an individual or a group that is lost or stranded in a remote or wilderness area, beyond the range of immediate assistance or rescue, where they must survive and support themselves without outside assistance for an extended period of time.

Communication for isolated personnel begins long before becoming anyone becomes isolated or is in need of rescue. All personnel traveling, working, and living in remote, hostile, and non-permissive areas should establish communications plans using the PACE methodology. Even in relatively "safe" areas, PACE plans should be developed in case of power outages, disruption of standard communications networks, civil disturbance, or the failure of other critical infrastructure.

PACE Communications Planning

PACE stands for **P**rimary, **A**lternate, **C**ontingency, **E**mergency and is a four-step method of ensuring that you can maintain communication with another person, group, or organization. PACE plans are specific to each communications link. The PACE plan that you have to ensure that you can communicate with your spouse / partner will almost certainly be different than the PACE plan you have to communicate with a family member who lives in a different state, and both of these plans will be different from a PACE plan designed to communicate with your base camp while hiking in some wilderness area. A basic example of a PACE plan might be:

- **Primary** – Cell-phone
- **Alternate** – Email
- **Contingency** – Radio
- **Emergency** – Satellite Messenger

Primary – Most people have a cell-phone. In the United States, as of June 2024, 98 percent of Americans owned a cellular phone of some type, with 91 percent of Americans owning at least one smartphone. (Pew Research Center, 2024)

We carry our cell-phones with us every day and as long as the cellular networks are up, we can communicate with others almost anywhere in the world. It makes sense then to designate our cell-phones as our primary means of communication. But, if for some reason the cellular network is down, or we are just in an area with no cellular signal, we would need an alternate means of communication.

Alternate – When the primary means of communication fails or is unavailable, we move to our alternate means of communication. Web-based email, such as Gmail or Protonmail, can be accessed from any place that there is an established Internet connection. Perhaps our cell-phone is lost or broken, but we can still access the Internet from home, a public library, or an Internet café. Email becomes our alternate means of communication, allowing us to communicate with anyone else who has a valid email address.

Contingency – When both our primary and alternate means of communication fail, we move to our contingency method of communications. A winter storm has knocked out power in our area and the cellular towers are down. But, our contingency method of communications – radio – still works. With a pre-coordinated frequency and contact times we can stay in contact with other without having to rely on commercial communications infrastructure, such as cellular networks and the Internet.

Emergency – When all else has failed, we move to our emergency communications method. In this case we are relying on a satellite messenger, such as the Garmin inReach or the Zoleo Satellite Communicator. This emergency communication might be just an exchange of text messages between you and a trusted friend, or might include activating the SOS function on the device, which will send an alert to both the rescue center and the emergency contacts listed in your account.

Your PACE plan should be adjusted for different circumstances and environments. For example, if you are going camping in an area that you know has no cellular service, you would not use your cell-phone as your primary communications method. From your campsite, maybe radio becomes your primary means of communication because you have tested it and know that you can easily make radio contact between your campsite and your home. Your alternate method is text messages using your satellite messenger. Contingency is that you hike into the nearest town where you can get a signal and make a call with your cell-phone. And, Emergency is the SOS button on your satellite messenger.

Each PACE plan will be unique to the parties involved, their capabilities, and to the communications environment. What is important however is that you have an established PACE plan with anyone with whom you need to stay in contact. PACE becomes even more important in areas with poor communications infrastructure. Remote wilderness areas likely have no cellular service, but you may be able to obtain Internet using a satellite-based service, such as Starlink. In hostile and non-permissive areas, with an increased probability of isolation, having an established PACE plan is critical, and in these cases, you must take security into consideration to ensure that your communications are not intercepted, jammed, or located (direction finding) by an adversary.

GOTWA Contingency Planning

GOTWA is a plan coordinated with a responsible party anytime that you are going to be away from your main group, and whenever you are traveling in a remote, hostile, or non-permissive area. GOTWA stands for…

Going Where?

Others Going with You?

Time You Will Be Gone? (Returning Not Later Than.)

What Should Be Done If You Don't Return on Time?

Actions – What Action You Plan to Take if Lost, Injured or Stranded.

When briefing GOTWA you let a responsible party know where you are going and what routes you plan to take to get there and get back. Are others traveling with you? If so, who are they? Estimate the time that you will be gone, and provide a not later than time for your return. If you don't return on time, what should the responsible party (the person you briefed your GOTWA plan to) do? And, what actions do you plan to take upon enemy contact – if something goes wrong what do you plan to do?

GOTWA is designed to be quickly and easily briefed, and should be used every time that you will be away from your main group. GOTWA ensures that if something goes wrong while you are away, someone will be aware that you are overdue or missing, and will take specific planned actions to locate you and render assistance if needed.

Dead Man's Switch

A dead man's switch is a switch that is designed to be activated or deactivated if the human operator becomes incapacitated, such as through death, loss of consciousness, or being bodily removed from control. Originally applied to switches on a vehicle or machine, it has since come to be used to describe other intangible uses... in our case here, it transmits an alert to your emergency contacts if we go missing or don't check-in on time.

The company Hiker Alert (https://hikeralert.com/) has a subscription service ($8.99 per year in 2025) that allows you to create an on-line profile to aid rescuers, and set emergency contacts to whom that information is sent if you schedule an outing and do not check in and cancel the pending alert before the time you have set for it to be

sent. Hiker Alert is a useful service that you should consider as part of your communications planning.

Many email services allow you to write an email and then set the date and time that it will be set to the addressees – Schedule Send. If your email provider allows you to schedule a future date and time for emails to be sent, you can create your own version of Hiker Alert. Write an email asking your emergency contacts to check on you, and schedule that email to send at some time after your planned return from an outing. If you return on time as planned, simply log into your email and delete the message before it sends. If, however, you don't return as planned, your emergency contacts (everyone you addressed the email to) will receive a notice that you are overdue and may need assistance.

Your email should contain everything in your GOTWA plan, as well as additional information that may be useful to responders in getting aid and rescuers to your location. This email (your dead man's switch) is a back-up to briefing your GOTWA plan to a trusted person, and leaving a copy of your plan with that person – it is not intended to replace GOTWA or other coordination that you make with others prior to travel.

If you use a scheduled send email as your 'dead man's switch' be sure that your email service stores the message on their servers after you prepare it. You shouldn't have to stay logged-in to your email for this to work. Before using scheduled send email for alerting others that something may be wrong, test it with each of your planned contacts, and of course let those emergency contacts know that you will be using this method of sending an alert if things go wrong.

It is often useful to schedule two emails. The first is a 'please check on me' email scheduled to send one hour after your planned return time. This gives you a little bit of a buffer after your planned return to cancel the email if it is not needed, and still alerts your contacts that something may be wrong if you a delayed more than an hour beyond your planned return time. The second email is an 'Urgent, I need help' type email that you schedule to send an hour after your initial 'please check on me' email. This alerts your contacts that there is very likely a problem and that you require some type of support or assistance.

Now, depending on where you are and what you are doing, you may want to adjust the timing of these scheduled send emails. Maybe, you send the 'please check on me' email four hours after your scheduled, and the 'Urgent, I need help' email the following day. Your own particular circumstances will dictate both when and if you want to use this type of a dead man's switch in your communications plan. But it is always an option that you can consider using.

DoD Communications Planning for Isolated Personnel

According to Department of Defense (DoD) CJCS Guide 5260 'A Self-Help Guide to Antiterrorism' (10 June 2013)

Communication Plans. **The number one priority for an isolated person is to contact friendly authorities to report their identity and location by using the established communications plan.** Document the communication plan on the Evasion Plan of Action (EPA). Communication plans should address both short-term and long-term communication with friendly forces. The plan should include radio, phone (cell or satellite) information, contact times, frequencies, and intentions.

Signaling for Recovery. Timely and effective signaling will greatly help efforts to report, locate, identify, support, and recover isolated personnel. The best location

information comes from the individual who is equipped with a survival radio, cell phone, or other communication device and trained to report their current position. The isolated person's participation in providing their location to recovery forces is by far the most accurate, efficient, and expedient means of locating their position for recovery. Another good source for determining location is if recovery forces locate a radio's signal or detect a visual signal. Recovery forces will look at the isolated person's EPA to determine their signaling intentions. Based on the information in the EPA, recovery forces can search areas and potentially authenticate the identity of the isolated person.

Communications and Signaling

Type	Day	Night	Report	Locate
Radio/Data Burst [Combat Survivor Evader Locator (CSEL), PRC-112/148/152, etc.]	X	X	X	X
Personal Locator Beacon (PLB)	X	X	X	X
Blue Force Tracker (BFT) (emergency code/message)	X	X	X	X
Cellular/Iridium Phone	X	X	X	X
Ground-To-Air Pattern Signal (ground-to-air or strip signal)	X		X	X
Laser (red or green)	X	X		X
MK-13/MK-124 Flares	X	X		X
Fire (International distress: three fires 100 feet apart in a triangle or line) (Smoke for day: rubber/oil for dark, live vegetation for white)	X	X		X
Smoke Grenade	X			X
Signal Mirror (directional)	X			X
Space Blanket	X			X
VS-17/Signal Panel	X			X
IR Strobe (MS-2000, Firefly, VIP, Inova, SureFire)		X		X
Glint Tape/Glo-Tape (IR)		X		X
CHEMLITE (visible/IR)		X		X

Technical Communication. Personnel should document their EPA with detailed information on available communication device(s) to include make, model, frequency, serial number, SIM card data, international mobile equipment identity (IMEI) or electronic serial numbers (ESNs). Personnel should attempt to contact friendly authorities by transmitting a distress call via any available communication device. Isolated personnel should be prepared to identify themselves, authenticate, and transmit their location when directed. Besides requiring batteries, there are other

potential issues when relying on radios or cell phones. Radios or cell phones may malfunction, sustain damage, become lost/stolen, or lose their programming/power. Cell phones have an additional connectivity concern in that they may be unable to obtain a cell tower's signal or are incompatible with a country's communication system. Personnel should anticipate these problems and prepare to overcome them.

Personal Locator Beacons (PLBs). PLBs are a family of hand-held devices that transmit distress signals on an internationally monitored frequency. PLBs are not the primary means for alerting recovery forces during an isolating event. Personnel should follow the communications plan, as annotated in their EPA, to determine the appropriate time to activate a PLB. If necessary, personnel should use PLBs to report their situation when other prescribed methods are not available or are not working. Personnel should only use a PLB when all other means of reporting are unavailable, exhausted, or ineffective. They only broadcast distress and homing signals. Personnel should annotate their PLB's unique identifier number in their EPA or other similar emergency action plan. This will greatly assist alerted recovery personnel in confirming whether a transmission is an actual report of an isolation event or an inadvertent alarm. When employing a PLB, the greatest probability of successful satellite reception occurs when a PLB has a clear view of the sky from horizon-to-horizon. They are capable of operating in an environment with less than a complete view of both horizons (e.g., a valley, canyon, on a mountainside, wooded area, near a chain link fence, nearby or inside buildings), but any such obstruction will reduce satellite reception capability and/or degrade the PLB's signal; however, even if reception is clear, some signal information may be delayed and take up to an hour and a half before it gets to the to the appropriate agency which can respond to an activation.

Visual Signals. Isolated personnel may find themselves in a nontechnical communication situation due to drained batteries, loss, damage, or confiscation of their radio. Communication plans should include alternate procedures for signaling when radio contact fails, is not feasible, or is not available.

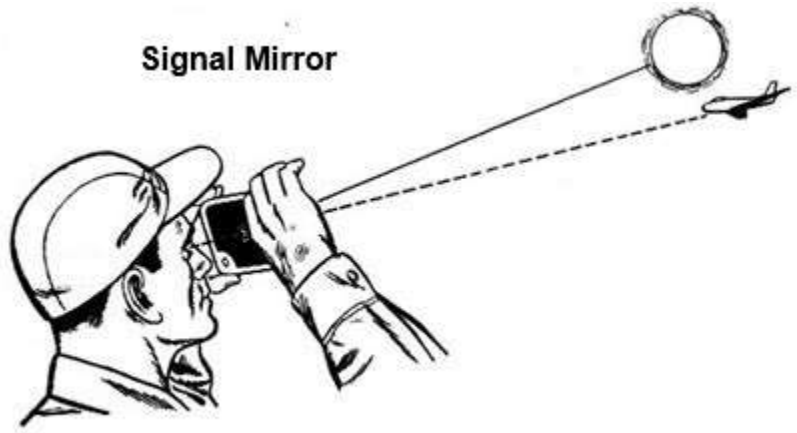
Strobes can be used at night to identify positions. If prior coordination has been conducted with supporting aviation units, strobes may be used to signal pilots. To reduce detection when used, strobe lights should be placed in holes so they can only be viewed from above. Strobes with infrared covers can be used if there has been prior coordination with the aircrew. (TC 3-21.60)

Glint tape is very sensitive infrared-reflecting cloth used for identification. Glint tape can be viewed with passive night-vision equipment and is highly visible to active infrared equipment. Evaders and downed aircrews use glint tape as an emergency night signaling device to mark their locations for infrared sensor equipped aircraft. Glint tape

is lightweight, durable, and very reliable. However, glint tape is susceptible to being obscured by smoke, dust, or precipitation. (FM 3-50.1)

Glow-in-the-dark tape - A special variety of glow-in-the-dark tape is used for the covert combat identification of troops, vehicles, and equipment. The most common use is to prevent fratricide. To the naked eye, the tape appears to be similar to black duct tape in both texture and finish, without a visible reflective glow. When illuminated with the infrared diode on standard night vision goggles, tape gives a bright reflection clearly visible up to 70 meters away. The bright reflection from an infrared laser can be seen up to 900 meters using a six-power night-vision scope.

Buzzsaw Signal – A Cyalume chem-light attached to a 3 to 4-foot length of cord and swung in circles creates an effective signal at night, visible both to aircraft and ground search teams. This buzzsaw techniques combines light and movement to attract attention of search teams. An infrared (IR) chem-light can be used to make your signal visible only to forces with night vision capabilities (although it should be noted that night vision is generally available in the commercial market, at reasonably affordable prices – so anyone may be equipped with night vision devices).



Mirrors are used to get the attention of an aircraft pilot during the day. Their use requires good visibility and little or no cloud cover in order to reflect the sun. Mirrors also can be used to transmit messages, if signals have been arranged.

Hold the mirror a few inches from face and sight at aircraft through hole. Spot of light through hole will fall on face, hand or shirt. Adjust angle or mirror until reflection of light spot in rear of mirror disappears through hole while you are sighting on aircraft through the hole in the mirror. Do not continue to flash mirror in direction of the aircraft after receipt of signal has been acknowledged.

Ground-to-Air Signals (GTAS). A GTAS is a supplemental system to radio or cell phone communications. They are non-directional signals that identify an individual's general location. Signal construction could consist of colored (parachute) panels, specially aligned radar reflective devices, glint tape, specially shaped IR reflectors, metallic trash (cans, foil, sheet metal, screen wire, vehicle parts), building debris, natural materials (e.g., sticks, logs, rocks, sod, dug or turned soil, vegetation), to make a visually recognizable or meaningful signal. Individuals should annotate the EPA with the type of signal they intend to use and the distance and direction they intend to travel in relation to all visual signals. Personnel should choose materials appropriate to the environment and those that will not degrade in weather. Isolated personnel may signal the approaching recovery asset by using a directional signal aimed towards the recovery asset to pinpoint the individual's specific location. Directional signals include mirrors, flashlights, laser lights, shielded IR lights, chem-lights and specially shaped IR reflectors. If isolated in a hostile environment, and in voice contact with a recovery force, personnel should employ non-directional signals, such as flares and smoke, only when directed. Isolated personnel may need to improvise signaling devices (car or bike mirror, polished metal, bright colored cloth, etc.) and become very creative to avoid enemy detection.

F	II	X	I	≫	K
Require food and water	Require medical supplies	Unable to proceed	Require doctor serious injury	Require firearms and ammo	Indicate direction to proceed
↑	I⟩	⊔	△	LL	L
Am proceeding in this direction	Will attempt take off	Aircraft badly damaged	Probably safe to land here	All well	Require fuel and oil
N	Y	JL	W	□	!
NO	Yes	Not Understood	Require mechanic	Require map and compass	Require signal lamp with battery and radio

If in doubt on what symbol to use or of the current situation, use this international symbol : **SOS**

Message Received and Understood

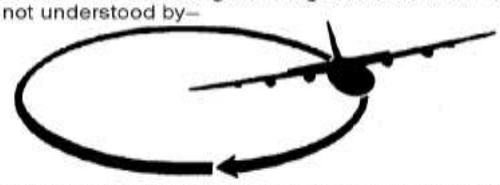
Aircraft will indicate that ground signals have been seen and understood by–

Day or moonlight: Rocking from side to side.

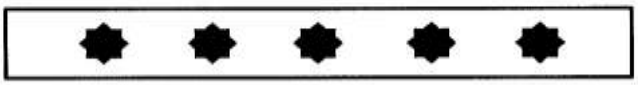
Night: Making green flashes with signal lamp.

Message Received But Not Understood

Aircraft will indicate that ground signals have been seen but not understood by–



Day or night: Making a complete right hand circle.



Night: Making red flashes with signal lamp.

Recovery. Availability of potential U.S., allied or regional recovery assets are dependent on the situation at the time of isolation; time, threats, and distance are limiting factors. Because of the long distances and lack of traditional recovery assets, it may take a significant amount of time to execute a recovery mission. **Personnel should plan to survive and evade unassisted for a minimum of 72-96 hours.** However, recovery may take longer. Isolated personnel must also be prepared for long-term unassisted evasion.

Personal Survival Kits. Creating and carrying a personal survival kit will augment any issued survival equipment in order to help an isolated person survive. Individuals must personalize their survival kits for the operating environment. Consider including the following items in a personal survival kit: water, shade tarp, [firearms and] ammunition, radio, personal locator beacon (PLB), satellite phone, commercial tracking device, maps, compass, and emergency signaling devices, local purchase cell phone, sun block, insect repellent, head net, space blanket, burlap, poncho, a mirror, infrared (IR) and visible lights (e.g.: Fire Flies, laser pointer, Micro Lights, Phoenix, chemical lights, etc.), 3'x3' bright colored cloth, 1 sq. inch of glint tape, knife or multi-tool, fire starter, candle, button compass, water purification tablets, three 1-gallon zip lock bags, large plastic leaf/trash bag (for water storage and protection from the elements), 100 ft. parachute cord, gloves, large needles, dental floss, safety pins, first aid items, and any needed medications. If extra clothing is included, it should be lightweight, windproof, waterproof, and appropriate for cultural, environmental, and seasonal conditions. An outer jacket and hat and sturdy local footwear could be useful for blending with the local population. Having a small or moderate amount of local and U.S. currency may be useful for purchasing supplies or materials. During pre-mission planning, personnel should consider the different survival situations when deciding what to pack in their personal survival kits. Personnel should also determine which items are necessary to retain in an emergency and which are expendable.

Evasion kits— (FM 3-50.1)

A basic evasion kit may contain the following items:

- Signal mirror.
- Infrared black glint tape with hook and pile tape fastener.
- Distress marker light with infrared filter.
- Emergency whistle.
- Signal panel.
- Compass.
- Chemical lights (infrared, blue, yellow, green, red).
- Global Positioning System receiver.
- Signal light (three infrared and two green).

Radio Watch – Net Control Station (NCS)

Many people plan to use radio as an alternate, contingency, or emergency means of communication. Radio can be a useful means of communication, but it requires a certain degree of planning and coordination to truly effective.

An important consideration for effective radio communication is that you must have someone with whom to communicate. That is, there must be someone listening for and prepared to respond to your radio calls. The idea that you can pull a radio out of your pack and begin calling for help, that that call will be heard by some random person monitoring the frequency, and that this random person will be able to provide you with assistance or will quickly relay your call for help to someone who can come rescue you is unlikely at best.

When you are relying on radios for communication it is best to have an established radio watch / net control station (NCS) where someone is monitoring the radio 24/7. Alternatively, a schedule for making radio contact at specific times allows personnel to send and receive messages every few hours, or at least once per day while in a remote area.

The individuals monitoring communications for radio watch / NCS should be skilled in handling messages, have access to sources of information (i.e. geographic, medical, and weather data) to answer questions from personnel in the field, and have access to resources to provide support and rescue to isolated personnel when needed. These resources need not be a full search and rescue team, but may be as simple as knowing which local towing company can do off-road recovery to pull someone out of a ditch during an overlanding trip, being able coordinate a pick-up at a new location, date and time when trip plans have changed, arranging for re-supply of personnel in the field, or being able to rely information from a nurse advice line for someone who has become sick or injured in the backcountry.

The Radio Watch / NCS should use tools such as the Voice of America Coverage Analysis Program (VOACAP) (https://www.voacap.com/) to determine which frequencies will support an area of operation during a specific period of time. Equipped with this analysis, teams can be sure that they are using frequencies that will allow effective communication from the field.

The radio watch / NCS not only monitors communications links, but also serves as a source of information for personnel in the field and coordinates access to resources and support when needed. Whomever is working as your radio watch / NCS should have access to your trip itinerary / EPA, and other information that may be needed to support you (such as information about your health concerns and required medications) should something go wrong in the backcountry.

Personal Radio Services

Citizens Band (CB) Channels & Frequencies							
License **Not Required** for Operations							
CH	Frequency	CH	Frequency	CH	Frequency	CH	Frequency
1	26.9650	11	27.0850	21	27.2150	31	27.3150
2	26.9750	12	27.1050	22	27.2250	32	27.3250
3	26.9850	13	27.1150	23*	27.2550	33	27.3350
4	27.0050	14	27.1250	24	27.2350	34	27.3450
5	27.0150	15	27.1350	25	27.2450	35	27.3550
6	27.0250	16	27.1550	26	27.2650	36	27.3650
7	27.0350	17	27.1650	27	27.2750	37	27.3750
8	27.0550	18	27.1750	28	27.2850	38	27.3850
9	27.0650	19	27.1850	29	27.2950	39	27.3950
10	27.0750	20	27.2050	30	27.3050	40	27.4050

- CB equipment must be certified per FCC Rules, 47 CFR Parts 2 and 95, Subpart D (47 CFR §95.961)
- Amplitude Modulated (AM) voice signals, the mean carrier power must not exceed 4 Watts. (47 CFR §95.967)
- Single Sideband (SSB) voice signals; peak envelope power must not exceed 12 Watts
- Authorized emission types: A3E, J3E, R3E, and H3E (47 CFR §95.971)

*Shared with the Remote Control Radio Service (RCRS), 47 CFR Part 95, Subpart C.
Other RCRS frequencies close to CB include: 26.9950, 27.0450, 27.0950, 27.1450, and 27.1950 MHz

General Mobile Radio Service (GMRS) Channels & Frequencies						
Personal Use Only - License **Required** for Operations Strictly Prohibited for use by NMAC on Wildfire Incidents						
Interstitial Channels				Main Channels		
5 watts ERP Max		0.5 watts ERP Max*		50 Watts Max		
CH	Frequency	CH	Frequency	CH	Frequency	Repeater Input Frequency
1	462.5625	8	467.5625	15	462.5500	467.5500
2	462.5875	9	467.5875	16	462.5750	467.5750
3	462.6125	10	467.6125	17	462.6000	467.6000
4	462.6375	11	467.6375	18	462.6250	467.6250
5	462.6625	12	467.6625	19	462.6500	467.6500
6	462.6875	13	467.6875	20*	462.6750	467.6750
7	462.7125	14	467.7125	21	462.7000	467.7000
		* Handheld Only		22	462.7250	467.7250

- GMRS frequencies are not authorized to transmit in Part 90 certified equipment.
- GMRS equipment must be certified per FCC Rules, 47 CFR Part 95, Subpart E (47 CFR §95.1761)
- GMRS shares the simplex frequencies for labeled as FRS, channels 1-22.
- Authorized bandwidth: 20 kHz for 462 MHz interstitial and 462/467 MHz Main Channels (47 CFR §95.1773)
- North of Line A / East of Line C: 462.6500, 467.6500, 462.7000, 467.7000 may not be used; small control stations limited to 5 Watts. *Nationwide Travel's assistance; if CTCSS is required try 141.3 Hz.

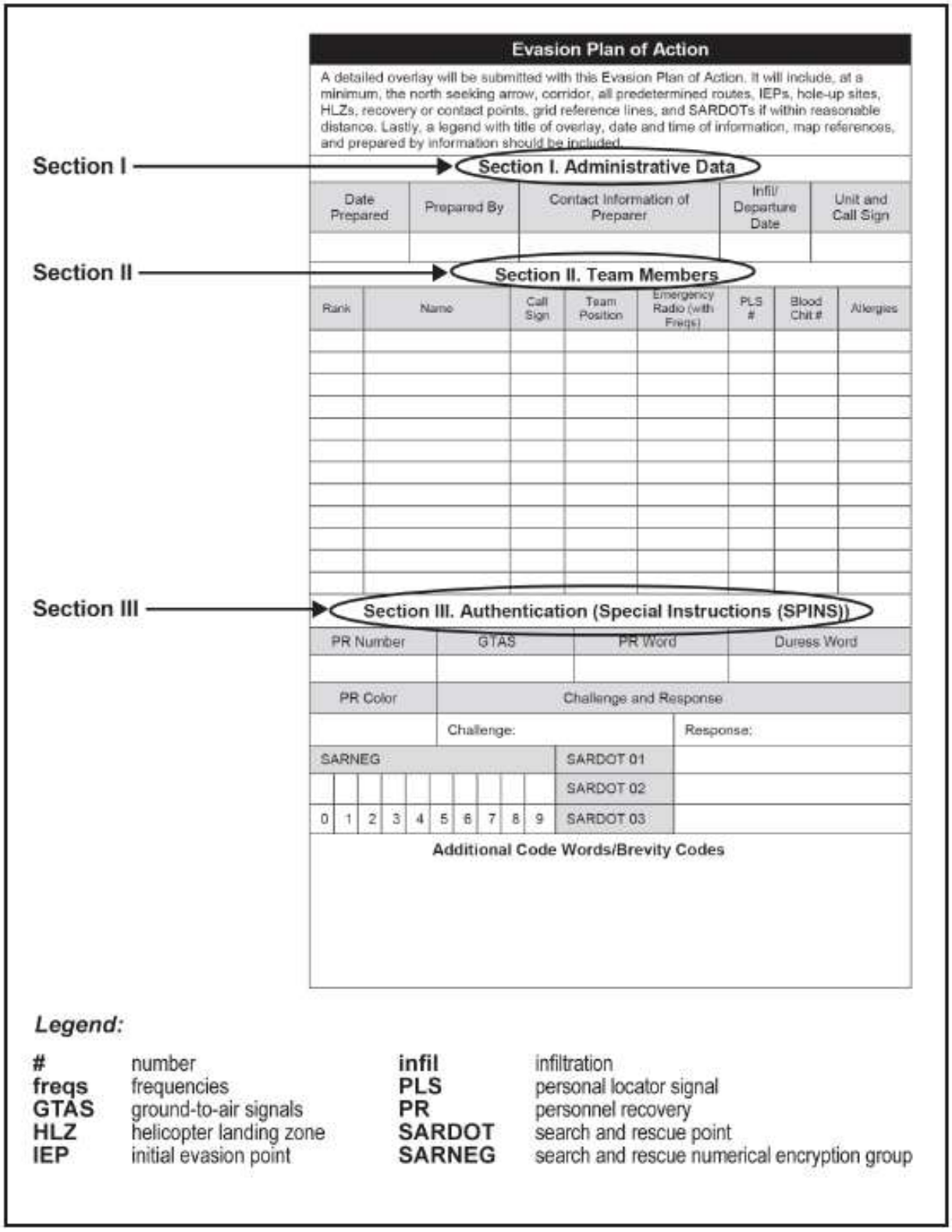
Multi-Use Radio Service (MURS) Channels					
License **Not Required** for Operations Strictly Prohibited for use by the NMAC on Wildfire Incidents					
CH	Frequency (MHz)	CH	Frequency (MHz)	CH	Frequency (MHz)
1	151.8200	2	151.8800	3	151.9400
4*	154.5700	5*	154.6000		
2 Watts Max					
- MURS equipment must be certified per FCC Rules, 47 CFR Parts 2 and 95 Subpart J (47 CFR §95.2761) - MURS frequencies are not authorized to transmit in Part 90 certified equipment. - Authorized emission types: A1D, A2B, A2D, A3E, F2B, F1D, F2D, F3E, G3E - Authorized bandwidth: 11.25 kHz (151.8200, 151.8800, & 151.9400) 20 kHz (154.5700 & 154.6000) - External gain antennas may be used (must be no more than 60 feet above ground, or 20 feet above the structure on which it is mounted. -Voice or data, except: No store-and-forward packet operation No continuous carrier operation No interconnection with the public switched network No use aboard aircraft in flight * Frequencies are shared with itinerant Industrial-Business operations.					

While the Amateur (Ham) Radio Service offers the greatest capability and flexibility in establishing communications for the prepared citizen, we should not overlook or discount the Personal Radio Services, including CB, FRS/GMRS, and MURS. CB, FRS, and MURS are all license free (licensed by rule), and while GMRS does require a license, there is no exam required – just a $35 fee paid to the Federal Communications Commission (FCC) for a 10-year license that covers your whole family.

Radio is an essential part of communications planning, and the Personal Radio Services are a great place to start expanding your communications capability. Even if everyone in your group is a licensed amateur radio operator, and if everyone you might want to communicate with is also licensed and authorized to use the amateur radio bands, you should still maintain the capability to communicate within the Personal Radio Services – if for no other reason than to take advantage of this additional available radio spectrum.

Even if you don't plan to use the Personal Radio Services as part of your own communications plan, there are almost certainly others in your area (both friendly and hostile forces) that are communication on these frequencies. So, at a minimum you should have the capability of monitoring / scanning all of the channels and frequencies in the Personal Radio Services.

Sample EPA Format



Evasion Plan of Action

A detailed overlay will be submitted with this Evasion Plan of Action. It will include, at a minimum, the north seeking arrow, corridor, all predetermined routes, IEPs, hole-up sites, HLZs, recovery or contact points, grid reference lines, and SARDOTs if within reasonable distance. Lastly, a legend with title of overlay, date and time of information, map references, and prepared by information should be included.

Section I → **Section I. Administrative Data**

Date Prepared	Prepared By	Contact Information of Preparer	Infil/ Departure Date	Unit and Call Sign

Section II → **Section II. Team Members**

Rank	Name	Call Sign	Team Position	Emergency Radio (with Freqs)	PLS #	Blood Chit #	Allergies

Section III → **Section III. Authentication (Special Instructions (SPINS))**

PR Number	GTAS	PR Word	Duress Word

PR Color	Challenge and Response	
	Challenge:	Response:

SARNEG										
0	1	2	3	4	5	6	7	8	9	

SARDOT 01

SARDOT 02

SARDOT 03

Additional Code Words/Brevity Codes

Legend:

#	number	**infil**	infiltration
freqs	frequencies	**PLS**	personal locator signal
GTAS	ground-to-air signals	**PR**	personnel recovery
HLZ	helicopter landing zone	**SARDOT**	search and rescue point
IEP	initial evasion point	**SARNEG**	search and rescue numerical encryption group

An evasion plan of action (EPA) is a predefined strategic plan used by military personnel when they are behind enemy lines, which outlines steps to evade capture and return to friendly lines. It includes details like routes, navigation methods, food and water sources, as well as communication procedures with friendly forces. This plan is tailored to individual missions, geographical location, and the skill levels of personnel involved.

1. Identification

a. Name and rank (for each crew or team member).

b. Mission number, aircraft or team call sign or identifier, crew or team position, type aircraft, call sign suffix, other.

2. Planned Route of Flight, Travel, and/or Delta Points or Way Points on File

a. If not on file, the route points must be described in the EPA for the approach route, target area, and withdrawal route.

b. Describe enroute emergency plans for each leg of the mission.

3. Immediate Evasion Actions and/or Intentions for the First 48 Hours, Uninjured

a. Hide near vehicles, aircraft or parachute landing site or area of separation from team (distance and heading).

b. Evade alone or link-up with crew or team (rally points).

c. Travel plans (distance, duration or time, speed, and other such details).

d. Intended actions and/or length of stay at initial hiding location.

4. Immediate Evasion Actions and/or Intentions, If Injured

a. Provide hiding intentions if injured.

b. Provide evasion intentions if injured.

c. Provide travel intentions if injured.

d. Provide intended actions at hiding locations if injured

5. Extended Evasion Actions and/or Intentions after 48 Hours

a. Destination (recovery area, mountain range, coast, border, FLOT).

b. Travel routes, plans, and/or techniques (either written and/or sketched).

c. Actions and/or intentions at potential contact or recovery locations.

d. Recovery/contact point signals, signs, and/or procedures (written out and/or sketched).

e. Back-up plans, if any, for the above.

6. Supplementary Information.

The following information should be completed with assistance from appropriate PR cell personnel, operations, signal, intelligence, and life support personnel as needed.

a. Communications and Authentication

(1) Word, number, color, and/or letter of the day, month, or quarter; SARDOT; SARNEG; duress code word; other (as applicable).

(2) Available communications and signaling devices: type and quantity of radios, programmed frequencies, PLS code, encryption code, quantity of batteries, type and quantity of flares, beacons, mirrors, strobe lights, other.

(3) Primary communication schedule, procedures, and/or frequencies (initial/extended contact procedures).

(4) Back-up communication schedule, procedures, and/or frequencies.

b. Other Useful Information

(1) SERE training completed.

(2) Weapons and ammunition carried.

(3) Personal evasion kit items.

(4) Listing of issued signaling, survival, and evasion kit items.

(5) Mission evasion preparation checklist.

(6) Clothing and shoe sizes, Resupply, etc.

(7) Signature of reviewing official.

While the above EPA Sample is clearly focused on military operations, a similar plan adjusted for prepared citizens in a civilian environment can be very useful for responders and rescuers coming to your aid if you find yourself lost, stranded, and isolated in some remote area.

WHERE DO I GO IF ISOLATED?
Hole-Up Site

Purpose

- Used when more time is required for rest; attend to medical issues; meet basic needs; signal
- Locate hole-up site once at Designated Area for Recovery (DAFR)

Provides

- Localized access to water and food
- Concealment—ground and air
- Listening and observation points
- Multiple avenues of escape
- Protection from environment
- Communication and signaling opportunities
- Safe distance from enemy positions and LOC
- Be wary of weather extremes in the area (i.e., flash floods in ravines and canyons)

While at site

- Establish contact in accordance with ISG or EPA
- Take precautions to ensure signaling devices do not compromise position
- Review plan of action; establish priorities
- Reassess situation
- Inventory equipment
- Determine specific location
- Improve camouflage

Move from hole-up site only if required because of enemy activity or to move to recovery site!

Wilderness Protocol

The Wilderness protocol calls for amateur (ham) radio operators in wilderness areas to announce their presence on, and to monitor, the national calling frequencies for five minutes beginning at the top of the hour, every three hours from 7 AM to 7 PM while in the backcountry.

The National Simplex Calling Frequencies for Amateur (Ham) Radio are:

FM: 52.525 MHz, **146.520 MHz**, 223.500 MHz, 446.000 MHz, 906.500 MHz

SSB: 50.125 MHz, 144.200 MHz, 222.100 MHz, 432.100 MHz, 902.100 MHz

The intent of the Wilderness Protocol is that amateur radio operators monitoring these simplex frequencies may be able to provide information to and relay messages for other operators who are beyond the range of radio repeaters. The primary frequency for the Wilderness Protocol is 146.520 MHz, FM, with other calling frequencies used on a secondary basis.

While the Wilderness Protocol was conceived to facilitate communications between amateur radio operators that are hiking or camping in uninhabited areas outside of repeater range, it should not be viewed as something just for hikers and campers. The Wilderness Protocol can and should be followed by all amateur radio operators anywhere that repeater coverage is unavailable.

Although the Wilderness Protocol was designed for amateur radio operators, there is nothing to prevent it from being used in other radio services. GMRS and CB radio operators can adopt a similar protocol, perhaps monitoring GMRS Channel 20 and CB Channel 9, at the same times as established for the Wilderness Protocol.

Any radio operator who has the ability to monitor multiple frequencies – amateur radio, GMRS, and CB – should do so. Programming these frequencies into a radio scanner to allow for constant monitoring is encouraged.

To use the Wilderness Protocol, you monitor your radio for five minutes from the top of the hour (i.e., 0700 – 0705) every three hours from 7AM – 7PM local time. You are listening for and responding to anyone who needs to make contact and pass traffic (send a message). During the monitoring window operators announce their call-sign if they have traffic to pass. With a large number of radio operators in an area following the Wilderness Protocol, it works fairly well. But, with few operators following the protocol it becomes less effective, and it still relies on making a random contact with someone who happens to be monitoring the national calling frequency. Radio operators are encouraged to follow the Wilderness Protocol when in the backcountry, but to also understand its limitations and recognize that having an established radio watch with someone you know and trust will always be a better option.

Repeaters

Whenever traveling it is useful to make a list of amateur radio repeaters along your route and at your planned destination. Assuming that you are a licensed amateur (ham) radio operator this gives you another communications option while traveling.

The standard reference for repeater information is the **Repeater Book** website: (https://www.repeaterbook.com/). Repeater Book provides world-wide repeater data on the website, in a mobile app, and in a printed manual in conjunction with the ARRL. Using this data, you can ensure that you have communications with others along your route, and you can also identify repeaters that are AllStar or Echolink enabled and thereby communicate over long distances (world-wide) using these repeaters.

AllStar (https://www.allstarlink.org/) is a network of Amateur Radio repeaters, remote base stations and hot spots accessible to each other via Voice over Internet Protocol. AllStar's primary use is as a dedicated computer node wired to your repeater or radio. Connections from Echolink, other VoIP clients and telephone calls are supported.

Echolink (https://www.echolink.org/) software allows licensed Amateur Radio stations to communicate with one another over the Internet, using streaming-audio technology. The program allows worldwide connections to be made between stations, or from computer to station, greatly enhancing Amateur Radio's communications capabilities.

Of course, if you have a direct Internet connection you have multiple communications options available to you. However, in wilderness areas with no cellular or Internet coverage, you still may be able to use your radios to connect to an AllStar or Echolink capable repeater. You then connect that repeater to a repeater in your home area that is being monitored by your '*Radio Watch*' and you have established a communications link.

You can install the DV Switch app (for AllStar) or the Echolink app on your smartphone and use these apps to communicate when you have a cellular data or Internet connection, but for tactical communications it is recommended that you plan to connect to these apps through repeaters using your radio.

Digital Mobile Radio (DMR), Digital Smart Technologies for Amateur Radio (D-STAR), and Yaesu System Fusion (YSF) are digital voice modes used in amateur radio. Each mode has its own linking systems and protocols across the Internet, but they can be bridged to allow communication between them. For instance, DMR can be bridged to YSF and D-Star using cross-mode setups on systems like Pi-Star (https://www.pistar.uk/).

These modes are often used by amateur radio operators, connecting through personal hotspots that provide then worldwide connectivity through devices such as the

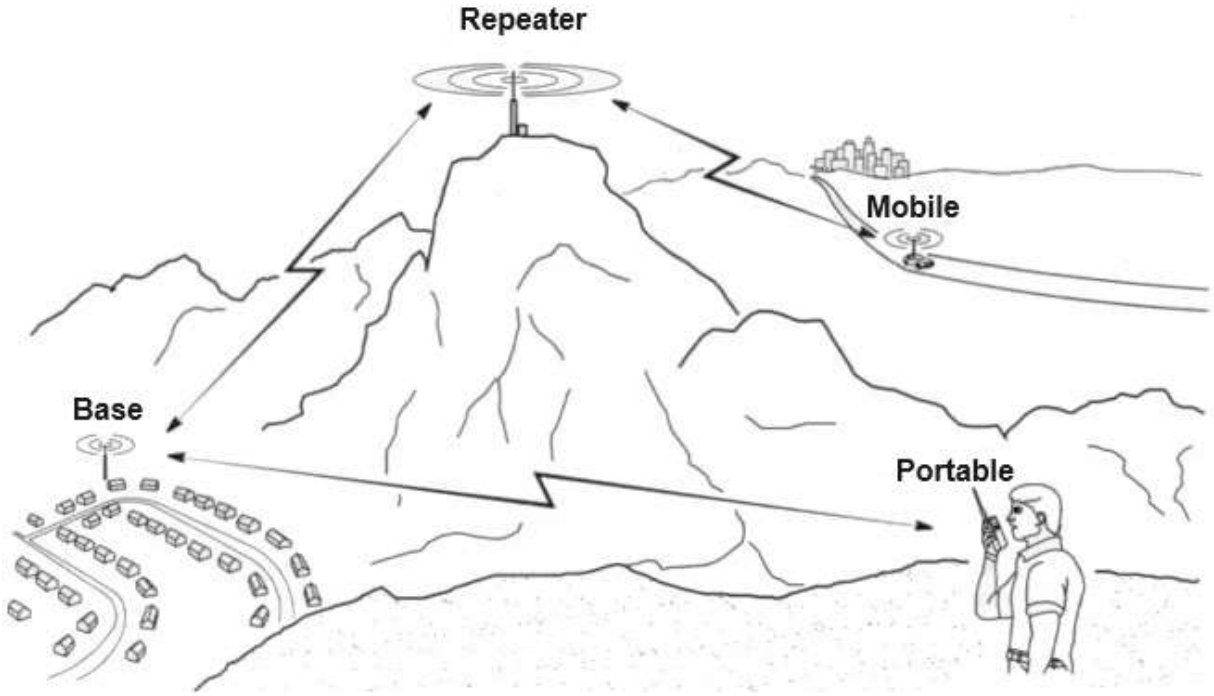
Open Spot by Shark RF (https://www.sharkrf.com/products/openspot4/). But as with AllStar and Echolink, these digital modes are also incorporated into repeaters that can be accessed using a compatible radio. If you are able to connect to a digital repeater and access a reflector / talkgroup you will be able to communicate with anyone else also connected to the same reflector / talk group, anywhere in the world.

The specific digital mode supported by a repeater will depend on the preferences of the repeater owners and operators, with one mode often being very popular in one area, and a different mode being more popular in another area. Before relying on a specific digital mode, determine which mode is most popular in your area and which repeaters support which modes.

Focus on repeaters with wide-area coverage. These repeaters are often located on mountaintops, in fairly remote areas themselves. It is these mountaintop repeaters that will likely give you the best coverage from the backcountry into surrounding towns and cities, or connections into Internet linked modes giving you world-wide communication possibilities.

It should be noted that all of these digital modes can be used in simplex (direct radio to radio communication) mode. This provides you with line-of-sight voice communication, as well as allowing digital messaging (SMS-type text messages). These digital messages can also be sent through Internet-linked repeaters. Unlike cellular networks which will store and forward messages, digital radio messages normally will not do this, requiring that the intended recipient of the message be connected to the reflector / talk group at the time the message is sent. However, once a SMS message has been received by the intended recipient's radio, it will be stored in the radio's memory until it is read and deleted. Thus, messages can be received without the need for an operator to be actively monitoring the radio – the radio only needs to be on and set to a common reflector / talk group.

Having a list of repeaters in your operational area, knowing their locations and coverage areas, and knowing what capabilities each repeater has is an important part of communication planning. Which repeaters have emergency / back-up power and how long can the function during a power outage? Do repeaters have autopatch capability, allowing you to use them to place a telephone call? Is a repeater linked to other repeaters, thereby expanding its coverage, or can it be linked by entering the proper control codes? Are the repeaters Echolink capable, and if so, what tones do you enter to connect to a distant Echolink node from that repeater?



Repeaters work by receiving a signal on one frequency and re-transmitting that signal on a different at a standard off-set. A radio set up to use repeaters automatically switches between the transmit and receive frequencies when you key and un-key the microphone. A repeater located well above the surrounding terrain (such as on a mountain or atop a tall building) has an improved line-of-sight footprint, meaning that the repeater can be heard over a wider area than someone transmitting from another location.

While a repeater may increase the area where your radio transmission is heard, repeaters can also be used to hide your actual location from radio direction finding. Use a directional antenna and low transmitting power to beam your signal directly to a repeater. The repeater receives and retransmits your signal omni-directionally and usually at a much higher power. Direction finding stations can easily locate the repeater location (which is probably already known), but unless the direction-finding station happens to be on the direct signal path between you and the repeater, they will have a much more difficult time locating your true position on the ground.

Simplex Repeaters – In addition to the common duplex repeater discussed above, there are also simplex repeaters that operate a bit differently. A simplex repeater (such as the one offered by Argent Data Systems) works by recording a transmission made on a specific frequency and then immediately replaying the recorded transmission on the same frequency.

Simplex repeaters are used to provide short-term coverage of an area. The simplex repeater is plugged into a radio (often a hand-held radio) and is placed at a location that overlooks an area. For example, a simplex repeater might be placed on a hilltop to provide coverage of the valley below during a day of hunting and fishing in a wilderness area.

More commonly however, simplex repeaters are used for radio voicemail, where a transmission is recorded and then played back at a later time when the simplex repeater receives the correct DTMF code. Radio voicemail is a very useful function for teams operating in remote areas, as messages can be passed without requiring a full-time radio watch / NCS.

Practice using repeaters, document their locations, capabilities and coverage areas, and test them often to ensure that they are still on-the-air and are available to support your communications needs.

Winlink Global Radio E-mail

Winlink (https://winlink.org/) is a worldwide radio messaging system that uses amateur radio frequencies and government frequencies to provide radio interconnection services that include e-mail with attachments, position reporting, weather bulletins, emergency and relief communications, and message relay. The system is built and administered by volunteers and is financially supported by the Amateur Radio Safety Foundation.

The Winlink system is open to all properly licensed amateur radio operators. The system primarily serves radio users without normal access to the internet, government and non-government public service organizations, medical and humanitarian non-profits, and emergency communications organizations. Duly authorized Military Auxiliary Radio System (MARS) operators may utilize the MARS part of the system.

Winlink connects to the Internet through common message servers (CMS), currently hosted by Amazon Web Services (AWS), but can also function in a radio-only mode (no Internet) or in a peer-to-peer mode where a direct connection is made between the sending and receiving station.

Winlink messages sent to or from at least one US-licensed station on amateur radio frequencies (meaning via RF only) are viewable in the ‘US Amateur Radio Message Viewer’ on the Winlink website for 21-days. This is done to comply with FCC regulations regarding openness within the Amateur Radio Service, but only applies to Winlink messages that pass through a Winlink Gateway. Radio-only and peer-to-peer messages are not recorded in the message viewer.

A significant advantage of Winlink is the ability to operate from remote and isolated areas. Winlink connections can be made using a simple laptop computer or smartphone to run the Winlink software, and a radio (even a hand-held (HT) radio) to transmit the message.

Emergency Frequencies

Amateur Radio Emergency Frequencies – According to the National Interoperability Field Operations Guide (NIFOG), Version 2.02, dated January 2025...

Emergency Center of Activity Frequencies for emergency communications networks in North/Central/South America and the Caribbean are encouraged to establish their operations within 20 kHz +/- of these frequencies (kHz): 3750 or 3985 LSB // 7060, 7240, or 7290 LSB // 14300 USB // 18160 USB // 21360 USB.

14300 USB is also the Maritime Mobile Service Network (https://mmsn.org/) common frequency, with daily nets held to assist mariners. ITU and FCC regulations allow a mariner in distress to use any means possible to attract attention to obtain help, including amateur radio frequencies.

It should be noted that there is probably not someone monitoring these frequencies 24/7 until these is a large-scale emergency or disaster, at which time HF emergency nets may be established on these frequencies.

APRS 144.390 MHz – If you have an APRS capable radio, set your Position Comment to "**EMERGENCY**" and send a beacon. This will trigger an alarm on all other APRS capable radios that hear your beacon. Operators hearing this alarm will see your location (grid coordinates) and your emergency status. They may then attempt to send you a message through the APRS system to determine the type of emergency and what type of assistance you need, and/or notify local emergency responders that an emergency beacon was received from your call-sign at the beaconed coordinates.

Marine VHF Channel 16 – The International Telecommunication Union (ITU) has established Marine VHF Channel 16 (**156.800 MHz**) as a distress, safety and calling channel, and it is monitored 24 hours a day by many coast guards around the world. Radio watchkeeping regulations advise all sea bound vessels to monitor channel 16, so if you are on or near navigable waterways (at sea, on the Great Lakes, etc.) an emergency call on 156.800 MHz will likely be heard by someone.

Aircraft Emergency Frequency 121.500 MHz – Flight regulations require that "aircraft shall continuously guard (monitor) the VHF emergency frequency 121.500 MHz. All aircraft in flight and airport towers are monitoring this frequency. If you have a radio capable of transmitting on the AM air band frequencies, emergency calls on this frequency will be heard by all aircraft in your area. **243.000 MHz** is the NATO / Military Aircraft Combined Distress and Emergency Frequency.

It can also be useful to have the 'tower frequencies' of major area airports programmed into your radio, as these frequencies are generally monitored 24/7.

Only use these frequencies in a true life or death emergency!

Satellite Communications

Satellite messenger devices, such as Garmin inReach, ACR Bivy Stick, Zoleo, Spot X, and others, allow users in remote areas beyond the range of cellular networks and radio repeaters to send and receive messages through satellites. Depending on the device you choose, you may need to pair the device with your cell-phone, while other devices operate as a stand-alone messenger. The devices that you pair with a cell-phone are smaller and lighter than stand-alone devices, while of course the stand-alone devices have the advantage of not requiring that you have a cell-phone to use them.

In cases where ultra-light weight is not a requirement, stand-alone satellite messengers are preferred as they build redundancy into your communications package (if your cell-phone is lost or destroyed, you can still use your stand-alone satellite messenger).

Each of these satellite messengers requires a monthly / annual subscription. Subscription costs in 2025 ranged from $11.99 for the most basic service to $49.99 per month for unlimited messaging. This subscription also includes an emergency SOS service, and may include position tracking that allows you to post your position to an on-line map. It's important to note that if your subscription is not paid the messaging function of these devices will not function. Even the SOS function will not work without a paid subscription.

In 2025, T-Mobile announced that it had partnered with Starlink to provide text messaging through satellites. T-Mobile uses a direct to cell technology, acting like cell-phone towers in space, thereby allowing users to connect from almost any place on earth. While this is still in its Beta-Testing phase, satellite communication with just your cell-phone is now a reality.

A satellite phone functions similarly to a satellite messenger, but also allows for voice communication. Satellite phones cost several hundred to a couple thousand dollars, and require a subscription plan, with calls costing around one-dollar per minute. If you must have voice communication from remote areas a satellite phone will provide it, but it can become expensive if you make long or frequent calls.

Starlink also provides a portable satellite device (Starlink Mini) that provides Internet access over satellite. In 2025, the cost for this service was $50 per month for 50 GB of service, or $165 per month for unlimited service. The Starlink Mini is larger than a cell-phone, but is still an easily carriable satellite / Internet router that you connect to your laptop computer to have Internet access from almost anywhere on earth.

Isolated Personnel (IP) with Communication Equipment

Survival Evasion Resistance Escape (SERE) Operations (AF Handbook 10-644) (27 March 2017) makes the following statements about Isolated Personnel (IP) with Communication Equipment...

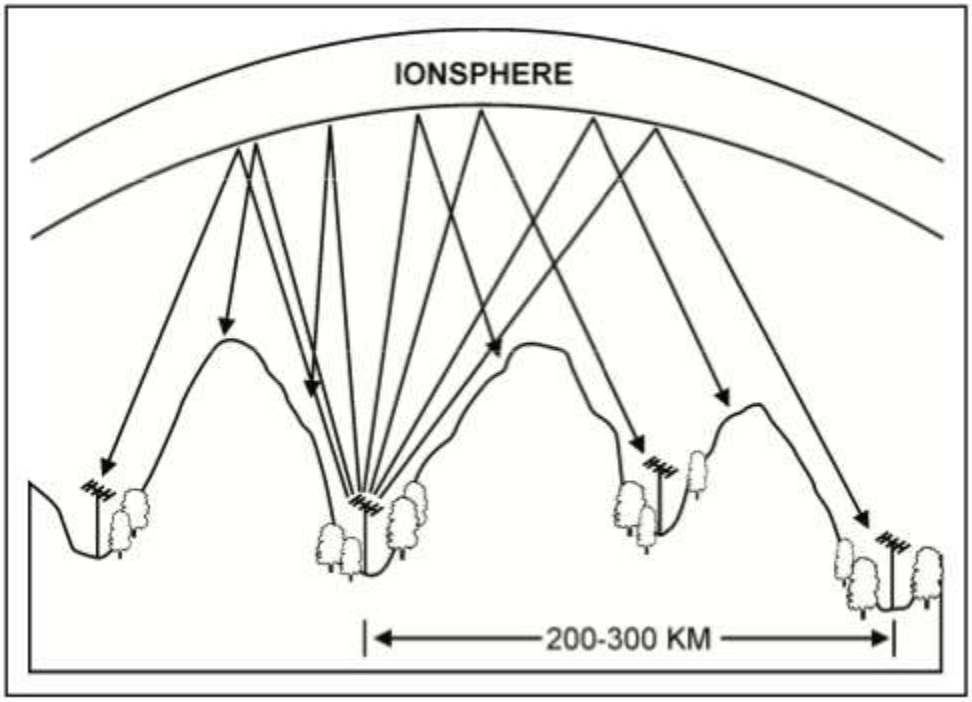
IP with communications equipment should follow the procedures outlined in their Evasion Plans of Action (EPA) and the Special Instructions (SPINS). Except for dire circumstances, do not attempt 'blind' radio communication outside the windows in your EPA's unless you can see (and positively identify) friendly aircraft or personnel. When contacted by rescue forces, speak in short bursts to reduce the possibility of having your position fixed by enemy forces, even if this means breaking up a single statement into several separate transmissions. It may be wise to cross-authenticate the rescue force via radio prior to making physical contact. Be prepared for the rescue force to ask you to move to a more suitable location for them to positively identify you. If you cannot move or signal from your position, consider vectoring the recovery force to your position. Understand that this is a high-risk technique for the rescue force, and may provoke hostile action if your posture is in any way non-compliant.

Before using radios and beacons, a few basic precautions should be observed. These will help obtain maximum performance.

- The best transmission range will be obtained when operating in clear, unobstructed terrain.
- Extending from the top and bottom of the radio antenna is an area referred to as the "cone of silence." To avoid the "cone of silence" problem, keep the radio/beacon antenna at a right angle to the path of the rescue aircraft.
- Never allow the antenna to ground out on clothing, body, foliage or the ground. This will severely decrease the effective range of the signals.
- To conserve battery power use in accordance with SPINS.
- If another radio or beacon is broadcasting, it may interfere with the radio or beacon transmissions.

"Knowledge of how to use communications equipment is a basic Soldier skill. Knowledge of, and the capability to use, personnel recovery related equipment such as a distress beacon is the key to a potential recovery. Low-tech communications systems augment electronic systems. Training of each Soldier in the use of visual signals such as colored panels, reflective mirrors, or signal fires is essential." (FM 3-50.1)

Near Vertical Incidence Skywave (NVIS)



NVIS propagation

Near vertical incidence skywave, or NVIS, is a skywave radio-wave propagation path that provides usable signals in the medium distances range — usually 0–650 km (0–400 miles). It is used for military and paramilitary communications, broadcasting, especially in the tropics, and by radio amateurs for nearby contacts circumventing line-of-sight barriers. The radio waves travel near-vertically upwards into the ionosphere, where they are refracted back down and can be received within a circular region up to 650 km (400 miles) from the transmitter. If the frequency is too high (that is, above the critical frequency of the ionospheric F layer), refraction is insufficient to return the signal to earth and if it is too low, absorption in the ionospheric D layer may reduce the signal strength.

The most reliable frequencies for NVIS communications are between 1.8 MHz and 8 MHz. Above 8 MHz, the probability of success begins to decrease, dropping to near zero at 30 MHz. Usable frequencies are dictated by local ionospheric conditions, which have a strong systematic dependence on geographical location. Common bands used in amateur radio at mid-latitudes are 3.5 MHz at night and 7 MHz during daylight, with experimental use of 5 MHz (60 m) frequencies. During winter nights at the bottom of the sunspot cycle, the 1.8 MHz band may be required. Broadcasting uses the tropical broadcast bands between 2.3–5.06 MHz, and the international broadcast bands between 3.9 and 6.2 MHz. Military NVIS communications mostly take place on 2–4 MHz at night, and 5–7 MHz during daylight.

NVIS propagation is simply sky wave propagation that uses antennas with high-angle radiation and low operating frequencies. Just as the proper selection of antennas can increase the reliability of a long-range circuit, short-range communications also require proper antenna selection. NVIS propagation is one more tool in the communicator's arsenal. To communicate over the horizon to person on the move, or to a station 100 to 300 kilometers away, the operators should use NVIS propagation. The ship's low take-off angle antenna is designed for medium and long-range communications.

When a non-NVIS antenna is used, a skip zone is formed. This skip zone is the area between the maximum ground wave distance and the shortest sky wave distance where no communications are possible.

Depending on operating frequencies, antennas, and propagation conditions, this skip zone can start at roughly 20 to 30 kilometers and extend out to several hundred kilometers, preventing communications with the desired station.

NVIS propagation uses high take-off angle (60° to 90°) antennas to radiate the signal almost straight up. The signal is then reflected from the ionosphere and returns to Earth in a circular pattern all around the transmitter. Because of the near-vertical radiation angle, there is no skip zone. Communications are continuous out to several hundred kilometers from the transmitter. The nearly vertical angle of radiation also means that lower frequencies must be used. Generally, NVIS propagation uses frequencies up to 8 MHz. The steep up and down propagation of the signal gives the operator the ability to communicate over nearby ridge lines, mountains, and dense vegetation. A valley location may give the operator terrain shielding from hostile intercept and also protect the circuit from ground wave and long-range sky wave interference. Antennas used for NVIS propagation need good high take-off angle radiation with very little ground wave radiation.

The ground wave portion of an HF radio wave becomes unusable at a distance of about 50 miles—and often at much less distance, depending on frequency, antenna type and polarization, and power output of the radio. The sky wave portion of the same radio wave, using standard antennas, is not reflected back to earth at a distance less than 100 miles. This can leave a gap of 50-plus miles where HF radio communication is ineffective (the skip zone). NVIS (Near Vertical Incidence Skywave) is a communication technique for high-frequency communications using antennas with a very high angle of radiation, often up to 90 degrees (straight up). When combined with a frequency below critical frequency that will be reflected off the ionosphere (generally in the 40-meter, 75/80-meter, and 160-meter bands), it provides for highly reliable communications in a roughly 200-mile circle around one's position – with no skip zone.

Weather Radio Broadcasts

NOAA Weather Radio "All Hazards" Broadcasts

NWR broadcasts National Weather Service (NWS) warnings, watches, forecasts and other non-weather related hazard information 24 hours a day. Channels WX1-WX7 are used in the US & Canada; channels WX8-WX9 are used for Canada Marine Weather broadcasts in some areas. These channels should be programmed as wideband FM (16K0F3E) receive only. Some radio manufacturers number the US weather channels in the order they came into use, others number them in frequency order. For programming in land-mobile radios, frequency order is recommended.

Weather Radio Broadcasts – Receive Only (WX1-WX7 US & Canada; WX8-WX9 Canada Marine Weather)						
WX1	WX2	WX3	WX4	WX5	WX6	WX7
162.400	162.425	162.450	162.475	162.500	162.525	162.550

Marine 21B	Marine 83B
WX8	WX9
161.650	161.775

Knowing the predicted weather for your area is essential for field operations. Most areas of the United States and Canada are covered by NOAA / NWS Weather Radio broadcasts, on the above listed frequencies. If your radios do not already have a built-in weather band, it is useful to program the above frequencies into your radios as Receive Only in order to be able to monitor weather information while in the field.

Weather forecasts can also be obtained by texting your state and public forecast zone number to the Alaska Weather Service at (907)539-5844, or by calling your local National Weather Service Office – for example Seattle at (206)526-6087.

Android Team Awareness Kit (ATAK)

ATAK (https://tak.gov/) is an Android smartphone geospatial infrastructure and situational awareness app. It allows for precision targeting, surrounding land formation intelligence, situational awareness, navigation, and data sharing. ATAK was originally developed by the Air Force Research Laboratory (AFRL) and is now maintained by the TAK Product Center (TPC), and is available for both military and civilian use.

Teams operating in the field can use ATAK to maintain situational and operational awareness – and this is where ATAK excels. Sharing maps, location data, messages, and targeting data with other team members, using ATAK over any shared network greatly enhances that team's capabilities in the field.

ATAK can also be used as a stand-alone app, taking advantage of its mapping and navigation features, but when running without a connection to other ATAK users it loses the advantage of team interaction, coordination, and planning. Other off-line mapping tools, such as OsmAnd (https://osmand.net/) may be just as effective as ATAK for mapping and navigation if you are not going to connect ATAK to other users.

Teams should connect with each other using ATAK through a shared TAK Server, via radio linking, within a common WiFi network, or by connecting to a mesh network such as Meshtastic (https://meshtastic.org/) or Reticulum (https://reticulum.network/).

Meshtastic is a decentralized wireless off-grid mesh networking LoRa protocol designed for low-power, long-range communication over unlicensed radio bands. An RNode is an open, free, and unrestricted digital radio transceiver that is part of the Reticulum system.

Meshtastic devices and Reticulum RNodes can – without integration with ATAK – provide communication between group members in a remote and isolated area. These devices connect with each other over the ISM Band (915 MHz in N. America) forming an encrypted mesh network.

Mesh Networks

A mesh network is a local area network in which the infrastructure nodes connect directly and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data to and from clients. This lack of dependency on any one centralized node allows every node to participate in the relay of information. Mesh networks dynamically self-organize and self-configure enabling dynamic distribution of workloads, particularly in the event that a few nodes in the mesh fail.

Meshtastic is perhaps the most popular mesh network being used for off-grid communication today, but there are other mesh networks that are becoming popular such as Reticulum and Meshcore (https://meshcore.co.uk/). All of these mesh networks use LoRa devices, which are then flashed (configured) with the software that support the chosen network type. Once a mesh network is established, users of the network can send messages to all members in the network or communicate directly with any individual member. This makes mesh networks ideal for communication within base camps, forward operating bases, and remote villages. Additionally, a mesh network can provide communication, that does not rely on commercial infrastructure, for groups in cities or other large populated areas. The communication across the mesh network is encrypted using AES-256, thereby providing a good amount of security for the content of messages sent over the mesh network.

The ground communication distance you can expect between node is ~1 to 3 miles in urban areas, and ~3 to 5 miles in open rural areas. Although under ideal conditions ranges well over 100 miles have been recorded between individual nodes. The advantage of a mesh network however is that you don't have to rely on direct communication between two distant nodes as messages will be relayed through all nodes in the network to find the best path to a distant node.

Mesh network devices all require a power source and, like a cell-phone, must be kept charged. But keeping the batteries of your device charged can be easily done with a small solar panel, or simply charge your mesh node in the same way that you recharge your cell-phone.

The basic LoRa board for building a mesh network device is very inexpensive, and completely assembled devices can be purchased from companies like SpecFive (https://specfive.com/), Rokland LLC (https://store.rokland.com/) and RAK Wireles (https://store.rakwireless.com/) for under $100.

There are many advantages of mesh networks for the prepared citizen, and teams should consider integrating these devices into their PACE plan.

SARDOT & SARNEG

Search and Rescue Dot (SARDOT)

- Geographic reference point known only to friendly forces that allows IP to pass location over unsecured net; direction is given in magnetic azimuth and distance from the SARDOT

SARDOT example:
"I am 250° and 15 clicks from Joe (SARDOT)."

- SARDOTs provided with PR code words
- Units may designate obvious terrain features for points of reference and incorporate into EPA

Search and Rescue Numerical Encryption Grid (SARNEG)

- 10-letter code word that allows IP to pass numbers over unsecured net and pass coordinates without regard for directional indicators; standard operating procedures (SOP) will normally direct coordinate format and SARNEG encoding procedures
- **SARNEG example:**

SARNEG	C	O	M	B	A	T	H	E	L	P
Encode	0	1	2	3	4	5	6	7	8	9

- **MGRS** coordinates 19TDJ2630801125 encoded as "19TDJMHBCLCOOMT."
- **Latitude/longitude** coordinates 263023N 0112517E encoded as "MHBCMBCOOMTO."

Isolated personnel may have to communicate over open (non-encrypted) radio channels. To allow more secure transmission of locations and to safeguard the numeric portions (grid coordinates, dates, times, etc.) of a message, the military uses SARDOT and SARNEG encryption.

A SARDOT is a designated geographic reference point from which a direction and distance is given to identify your general location. If you are due East of a SARDOT named "Hound" you could say over an open frequency that you are 90-degrees and 11-

kilometers from Hound. This would identify your general location to anyone who knew the location of SARDOT “Hound”, but to anyone listening without knowing where “Hound” is located all they could determine is that you are 11-kilometers East of somewhere – but that somewhere could be anywhere.

Each SARDOT should be an easily located and identified feature on the map, and on the ground, and specific enough to allow a bearing to be taken to that specific point. Using a water tower on a hilltop as a SARDOT might be a good choice, but using a city as a SARDOT would not as the location is far too general (what part of the city is the SARDOT referring to?).

“Where the isolated person has a communications link with friendly headquarters or other units, the use of an azimuth or bearing to prominent objects such as a terrain feature or the sound of combat operations can help to locate the individual. This method also includes shooting a compass azimuth to the impact of mortar, artillery, or other indirect fire to help recovery forces to pinpoint an isolated person.” (FM 3-50.1)

To provide a specific grid coordinate for your location, you could use SARNEG encryption. SARNEG is a simple substitution cipher, based on a 10-letter key word (with the letters numbered 0-9). The above graphic shows an example of encrypting a grid coordinate using SARNEG. It should be understood however that SARNEG is not a highly secure means of encryption. SARNEG is simply used to delay someone monitoring your communications from immediately identifying your location or other key information contained in the numeric portions of a message.

SARNEG has the advantage of being able to be used with nothing more than a memorized key word. SARNEG is used when you don’t have other more secure methods of encryption and when you must transmit in the clear – perhaps to link-up with an inbound rescue force. By the time a hostile force can determine your location protected by the SARNEG encryption, you will have linked-up with the rescue force and exfiltrated from the area.

SARNEG is a means of short-term, emergency, encryption and should not be used to protect routine radio traffic. For routine encryption of numeric portions of a message a system like DRYAD is recommended.

DRYAD Numeral Cipher/Authentication System

	ABC	DEF	GHJ	KI	MN	PQR	ST	UV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
A	ERSQ	WOJ	NKI	PB	YD	MTA	GU	HV	XF	LC
B	GJNH	ULF	EKA	OY	VB	STC	DI	QP	WR	XM
C	DAFH	CUB	TKM	OR	NE	GXQ	VY	IL	SP	JW
D	RMXF	IVO	TQY	WS	JP	LBD	CK	GE	HU	NA
E	IATL	DVO	SWX	MH	KQ	EYF	RN	BC	PU	JG
F	RCMX	AGO	TIE	NF	PH	YDB	QV	LK	UJ	SW
	ABC	DEF	GHJ	KI	MN	PQR	ST	UV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
G	TYKN	AHE	VUQ	IM	FD	RCW	BO	XP	JS	LG
H	AHOG	CKS	PNU	BR	DT	MYX	EQ	FL	VW	JI
I	OWGJ	SXC	DAP	RE	LY	QUF	MV	NB	TH	IK
J	YNAT	GBD	LOF	EJ	RS	MIK	WH	PQ	XU	VC
K	LYQE	UVN	JIC	HM	AG	KTP	DW	OX	SR	FB
L	GQCN	HUI	SMR	JB	FO	XWY	VT	EA	KL	PD
	ABC	DEF	GHJ	KI	MN	PQR	ST	UV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
M	CLUR	TJN	VAF	EX	DW	QKH	MP	GB	YI	OS
N	RPJU	QHX	CTN	OW	MA	KBV	EL	IG	SD	FY
O	QTOY	XMK	AWN	RJ	EF	PLS	DV	HB	CI	UG
P	PWMR	IEJ	ADK	GH	TS	QYC	ON	BU	LF	VX
Q	JRDA	QFN	BOI	SM	WH	KCX	GP	VL	YT	EU
R	MPBR	WXC	VJD	UN	KG	HQF	SE	LI	AY	TO
	ABC	DEF	GHJ	KI	MN	PQR	ST	UV	WX	YZ
	0	1	2	3	4	5	6	7	8	9
S	YPFV	DLU	QKT	HR	EO	ASI	CG	XN	MJ	WB
T	NCRT	DOG	UYX	BE	WJ	FSH	QP	LI	VM	AK
U	EBJR	IHV	YGL	AQ	NC	WPS	UX	KD	FO	TM
V	JOTC	VAB	DIR	FS	LW	QHU	EP	XY	KN	GM
W	AOCN	WJL	KDB	PI	RV	FGQ	UH	SM	XT	YE
X	SVHC	EML	YOA	GU	DK	FXI	JN	WT	PB	RQ
Y	EBOH	STL	FIM	GW	PY	JVA	UR	DN	KX	QC

The DRYAD Numeral Cipher/Authentication System is a simple, paper cryptographic system employed by the U.S. military for authentication and for encryption of short, numerical messages.

A DRYAD cipher sheet contains 25 lines or rows of scrambled letters. Each line is labeled by the letters A to Y in a column on the left of the page. Each row contains a random permutation of the letters A through Y. The letters in each row are grouped into

10 columns labeled 0 through 9. The columns under 0, 1, 2 and 5 have more letters than the other digits, which have just two each.

While somewhat crude, the DRYAD Numeral Cipher / Authentication System has the advantage of being fast, relatively easy and requires no extra equipment. The presence of more cipher-text columns under the digits 0, 1, 2 and 5, is intended to make ciphertext frequency analysis more difficult. But much of the security comes from keeping the cryptoperiod short. A new DRYAD table is used every day, and in nets with a lot of traffic the DRYAD table may be changed as often as every six hours.

DRYAD can be used in two modes, authentication or encryption.

DRYAD Authentication - For authentication, a challenging station selects a letter at random from the left most column followed by a second (randomly selected) letter in the row of the first chosen letter. The station being challenged would then authenticate by picking the letter directly below the row and position of the second letter selected.

DRYAD Encryption - The second mode is used to encrypt short numeric information (such as map coordinates or a new radio frequency). The coder arbitrarily selects two letters at random. The first letter designates a row in the current active page. The second one is used similarly to the authentication mode, except that the letter immediately to the right is selected. This selected letter is called the "SET LETTER."

Numbers are enciphered one digit at a time. A ciphertext letter is chosen from the selected row (the row designated by the SET LETTER) in the column under the plain text digit. If the digit occurs more than once in the number, the coder is instructed to choose a different letter in the same column. All the digits in a single plaintext number are encoded from the same row.

As an example, using the above DRYAD table, to encrypt the number 867-5309 an operator could send the message “I Set: Foxtrot Charlie” (this designates row M). “I Send: Yankee, Mike, Bravo, Kilo, Echo, Lima, Oscar” (YMBKELO).

DRYAD tables can be created by generating randomly ordered alphabets and then formatting the tables as shown above. Websites such as random.org claim to provide truly random data. The pseudo-random generator and spreadsheet formatting in MS Excel allows for rapid generation of DRYAD tables. Operators will have to weigh the advantages of rapid generation and formatting of DRYAD tables against the security of the pseudo-random generator (the Mersenne Twister algorithm) used in programs like MS Excel.

A DRYAD table for each day of the planned mission should be carried by operators in the field, thereby allowing for message authentication and encryption of the numeric portions of messages to safeguard that information should it be intercepted.

Sample Brevity Matrix

	A	B	C	D	E	F	G	H	I	J
1	North	Use UHF	Not Serious	Truck	Grid	Bogey on Net	Fastrope	VAPI	Send MRE	SPIE
2	Jeep	Low Band	Use VHF	Time Check	Need CAS	Need ARTY	Send 40 mm	Comm . Site	Trench Line	E&E
3	Smith 2435 O+	Jones 9735 O-	Assem. Area	No. of Troops	Troops Dug In	Para. Resupp. Needed	NATO Format	CH-46	Adams 0274 A+	Ottis 7395 AB+
4	3rd Team	Insert Compl.	South	Extract Time	At Obj.	Abort Mission	Hot LZ	Flash	HMM WV	Observe
5	Priority	Foot	120' Rope	Letters	BDA	Chem. Lights	Man injured	UH1N	West	Comm. Change
6	High Band	Scuba	Today' s Freq.	CH-53	Send 5.56LK	Linkup Aborted	On the Move	Insert. Compl.	2nd Team	Extract Grid
7	1st Team	AT ORP	No. of Troops	Helo. Cast	Send Batt.	Cache Location	More To Follow	Time Check	Send 5.56	No-Fire Area
8	UH-60	DZREP	ALZRE P	POSRE P	Alt.Freq.	SPOTREP	East	DELT AREP	BRIDG EREP	TUNNE LREP
9	Area Recon.	FORD REP	Check-oint	SITREP	Ambush	Point Recon.	Observe	Halt	Move to	HQ Element
10	Need Batt. Type	Bunker	Low Band	Need Camera Film	Send Frag. Grenad e	Emerg. Extract	Photo Grid	Strobe	Naval Gunfire	Linkup

Note: This should be read up then to the right. An example is, "A1E this is D3K, 4D over." (What time is extract?) "D3K this is A1E, 0700 out." (0700.)

The USMC Reconnaissance Reports Guide - MCRP 2-10A.7 (12 April 1998) recommends using a brevity matrix to shorten on-the-air transmission times. Only those items that pertain to a particular reconnaissance patrol are added to the matrix. This avoids filling the brevity matrix with information that is of no use, and keeps the matrix small enough to allow it to be quickly and easily used by operators in the field.

The American Radio Relay League's (ARRL) National Traffic System (NTS) in conjunction with Radio Relay International (RRI) has developed a brevity list, a series of numbered messages, for some of the more common texts sent during emergencies and holiday seasons. (https://nts2.arrl.org/numbered-texts/) You may want to include all or some of these numbered messages when creating a brevity list to use within your own team or group. The first twenty ARRL/RRI numbered messages are listed below by way of example (the complete list is available on the above listed web-site).

1 **ONE** Everyone safe here. Please don't worry.

2 **TWO** Coming home as soon as possible.

3 **THREE** Am in _____ hospital. Receiving excellent care and recovering fine.

4 **FOUR** Only slight property damage here. Do not be concerned about disaster reports.

5 **FIVE** Am moving to new location. Send no further mail or communication. Will inform you of new address when relocated. Will contact you as soon as possible.

6 **SIX** Will contact you as soon as possible.

7 **SEVEN** Please reply by Amateur Radio through the amateur delivering this message. This is a free public service.

8 **EIGHT** Need additional _____ mobile or portable equipment for immediate emergency use.

9 **NINE** Additional _____ radio operators needed to assist with emergency at this location.

10 **TEN** Please contact _____. Advise to standby and provide further emergency information, instructions or assistance.

11 **ELEVEN** Establish Amateur Radio emergency communications with _____ on _____ MHz.

12 **TWELVE** Anxious to hear from you. No word in some time. Please contact me as soon as possible.

13 **THIRTEEN** Medical emergency situation exists here.

14 **FOURTEEN** Situation here becoming critical. Losses and damage from _____ increasing.

15 **FIFTEEN** Please advise your condition and what help is needed.

16 **SIXTEEN** Property damage very severe in this area.

17 **SEVENTEEN** REACT communications services also available. Establish REACT communication with _____ on channel _____.

18 **EIGHTEEN** Please contact me as soon as possible at _____.

19 **NINETEEN** Request health and welfare report on _____. (State name, address and telephone number)

20 **TWENTY** Temporarily stranded. Will need some assistance. Please contact me at _____.

Encryption & Field Ciphers

Other encryption methods, such as the One-Time Pad (OTP) Cipher (see: Secure Communications with the One-Time Pad Cipher -by Dirk Rijmenants (27 February 2022)) can provide much greater security for the content of a message, but are also more difficult for isolated personnel to use in the field. Historical pen & paper field ciphers, such as 'Turning Grille', 'Vigenère', and 'Playfair', do not offer sufficient security for modern day use, and should be avoided.

U.S. Army Field Manual, FM 34-40-2, Basic Cryptanalysis (September 1990) states: *"Small codes can be conveniently printed in the form of a small coordinate matrix system. Typically, 10 by 10 or larger, matrix codes, also known as code charts, can contain letters, numbers, and a small vocabulary of words. They are very easy to use, and communicators can be trained in their use very quickly and easily. They also offer more security than most simple ciphers."* (para 14-3)

Personnel going into areas where there is an increased possibility of isolation and the need to transmit sensitive information over an unencrypted frequency might be provided with code charts as part of their communications plan.

	C,D	E,H	F,I	J,K	T,L	M,O	U,V	Y,G	Z,N	P,Q	X,R	W,S	B,A
M,H	### Action, ive, ivity, s	## Addition, al	15 Advance, d, ing, s	45 After	A Aggressor, ive (ly), s	AD Air	Spell/fig. Begins	AL Airborne	AM Aircraft/ Airplane, s	AN Ammunition	AND Antiaircraft	AR Antitank	ARE Area (of)
T,Q	## Armor, ed	## Arrive, al, d, ing, s	16 Artillery	5# Assemble, d, ing, s	AS Attack, ed, ing, s	AT Attempt, ed, ing, s	B Azimuth (in degrees)	BA Battalion, s	BE Battery, ies	BY Begin/start, ed, ings, s	C Bomb, ed, er, ing, s	CA Bridge, d, ing, s	CAN Capture, d, ing, s
K,Z	# Casualty, ies,	## Command er, ing, s	17 Communicate, d, ing, ion, s	55 Company, ies	CE Complete, d, ing, ion, s	CH Concentrate, d, ing, ion, s	CO Contact, ed, ing, s	D Coordinate, d, ing, ion, s	DA Corps	DAY Counterattack, ed, ing, s	DE Cross, ed, es, ing	DI Defend/de-fense, s (of)	DO Delay, ed, ing, s
O,L	1 Destroy, ed, ing, s	## Detach, ed, ment (of), s	18 Dispose, al, d, ition, s	E Division, s	EA Dump, s	ED East (of)	EE Encounter, ed, ing, s	EN Enemy' s	ENT Engineer, s	ER Enlisted Man/Men	ERS Equip, ment, ped, ping	ES Escape, d, ing, s	EST Estimate, d, ing, s (of)
R,X	2 Expect, ed, ing, s (of)	## Fight, er, ing, s	19 Fire, d, ing, s	ET Flank, s	F Force, d, ing, s	FO Forward	FOR Friend, ly	G From	H Front, al, s	HA Fuel, s	HE Gun, s	I Has/have	IL Headquarters
S,P	3 Heavy, ily	## Hill, s (No.)	2# Hold, ing, s/held	IN Hostile, ity, ities	ING Hour, s	ION How	IS Identify, ied, ies, ing, ication	IT Immediate, ly	IVE Infantry	J Inform, ation, ed, ing, s	K Install, ation, ed, ing, s	L Junction, s (of)	LA Land, ed, ing, s
W,N	4 Large	## Left (of)	21 Line, s (of)	LE Locate, d, ing, ion, s	LI Machine gun, s (nest)	LO Main	LY Map, ped, ping, s	M Mechanize, d	MA Message, nger, s	ME Mile, s (from), (to)	MENT Mine, d, ing, s	MI Mission, s	MY Morning
A,B	5 Mortar, s	## Move, d, ing, ment, s	22 Near	N Night	NA No/not/no-thing/negat	ND North (of)	NE Number, s, (of)	NI Objective, s	NO Observe, ation, d, ing, s	NOT Occupy, ied ies, ing	NT Officer, s	O Operate, d, ing, ion, s	OF Order, ed, ing, s
C,E	6 Over	1# Patrol, led, ling, s	23 Penetrate, d, ing, ion, s	ON Plan, ned, ning, s (to)	OR Platoon, s	OU Point, ed, ing s	OUR Position, s	P Post, ed, ing, s	PE Prepare, d, ation, ing, s	Q Prisoner, s	OU Proceed, ed, ing, s, ure	R Radio, ed, s	RA Railway/ Railroad, s
I,G	7 Ready (for) (to)	11 Rear	25 Receive, d, ing, s/receipt	RE Reconnais-sance	RED Refer, ence, red, ring, s (to)	RES Regiment, al, s	RI Reinforce, d, ing, ment, s	RO Replace, d, ing, ment, s	RS Report, ed, ing, s	RT Request, ed, ing, s	S Require, d, ing, isition, s	SA Reserve, d, ing, s	SE Ridge, s
D,J	8 Right (of)	12 River/ Stream	3# Road, s/ Route, s	SH Scout, ing, s	SI Section, s/ Sector, s	SO Send, ing, s/sent (to)	ST Shell, ed, ing, s	T Small/ Small arms	TA South (of)	TE Squad, s	TED Strength, s (of)/strong	TER Stop, ped, ping, s	TH Supply, ies (of)
F,V	9 Support, ed, ing, s	13 Tank, s	35 Target, s	TI Today	TION Tomorrow	TO Tonight	TR Troop, s	U Truck, s/ Vehicle, s	UN Unit, s (of)	US Until	V Urgent, cy, ly	W Vicinity (of)	WE Water
U,Y	91 West (of)	14 What/who	4# When	X Where	Y Will	Z With	Spell/fig. Ends	Period . Withdraw, al, ing, s	Comma , Woods	Colon : Yard, s (from), (to)	Smicln ; Yesterday	Dash — You, r	Paren ( ) Zone. s (of)

Figure 14-1. Sample code chart.

"One type of code chart places two plaintext values in each cell—an upper value and a lower value. The lower values are all words. The upper values are all numbers,

letters, or syllables. Two of the cells are set aside as shift values to indicate whether to read the upper values or lower values in the code groups that follow. A sample chart of this type is shown in Figure 14-1. This example uses letters for coordinates, and has variants on each row and column. The word ARTILLERY, for example, could be encoded as TF, TI, QF, or QI. The cells MU and UU are begin and end spell indicators. The bottom values in each cell are used until a begin spell group is sent. Then the top values are used until the end spell group is used to shift back to the lower values."

Groups of prepared citizens may choose to develop code charts similar to the one shown in Figure 14-1 from FM 34-40-2. Unless used in a military context, words like Artillery should be replaced with words more likely to be used by the group in their operational environment. Once a group code chart is developed, the key letters on the outside of the matrix can be re-ordered / changed from time to time to help maintain security of the code.

Encryption Prohibited - The Federal Communications Commission (FCC) in the Code of Federal Regulations (CFR), Title 47 § 97.113 — lists as "Prohibited transmissions," the Federal Communications Commission (FCC) "messages encoded for the purpose of obscuring their meaning." While Part 97 applies to the Amateur Radio Service, similar regulations prohibit encryption in the Personal Radio Services, which includes CB, FRS, GMRS, and MURS.

While strong encryption will protect the content of your message, encryption – especially on frequencies assigned to radio services where encryption is prohibited – will attract attention. Other radio operators may make note of your violation of FCC regulations, and government agencies may assume that your use of encryption is an effort to commit or facilitate crimes. It should be noted that on 17 January 2021, the FCC published a Public Enforcement Advisory highlighting this concern.

> *The Enforcement Bureau (Bureau) of the Federal Communications Commission has become aware of discussions on social media platforms suggesting that certain radio services regulated by the Commission may be an alternative to social media platforms for groups to communicate and coordinate future activities. The Bureau recognizes that these services can be used for a wide range of permitted purposes, including speech that is protected under the First Amendment of the U.S. Constitution. Amateur and Personal Radio Services, however, may not be used to commit or facilitate crimes. Specifically, the Bureau reminds amateur licensees that they are prohibited from transmitting "communications intended to facilitate a criminal act" or "messages encoded for the purpose of obscuring their meaning." 47 CFR § 97.113(a)(4).*

While encryption may still be needed in some circumstances, and it can be a valuable tool in radio services where it is allowed (i.e., PLMRS / Business Radio), when used in radio services where it is prohibited, encryption may cause more problems than it solves. Encryption will almost certainly attract unwanted attention.

Signature Management

Communications planning for isolated personnel should focus on signature management, techniques to reduce electromagnetic (EM) emissions, and to create low probability of detection (LPD) communications nets. It's best when those attempting to intercept and exploit your communications simply find no signals to work with. The enemy is always listening, but if he cannot hear you, he cannot exploit you.

Something as simple as using digital modulation (i.e., D-STAR, DMR, P25) can prevent those with analog receivers from understanding your communications, although they will still know that a signal is present. But by sending that same message as a digital text (SMS-type) message it may be missed entirely, in the few seconds it takes the text to transmit, by someone scanning the bands for signals.

The Ten Commandments to Reduce EM Emissions

	Technique	Guidelines
1.	**TALK Less**	TALK **less**. TRANSMIT only **mission-critical** information. TALK **short**. TALK **correct**.
2.	**SCHEDULE Less**	MINIMIZE required **reports**. SCHEDULE comm **windows**.
3.	**MOVE**	MOVE **units**. MOVE **radios**. When in doubt, MOVE.
4.	**CHAT**	CHAT. Do NOT **call**. CHAT reports, requests, and brevity codes.
5.	**SIGNAL**	SIGNAL **movement**, **tactical action**, and **convoys** with one-arm hand and arm signals.
6.	**WIRE**	COMMUNICATE between stationary positions with **comm wire** and field phones.
7.	**MASK Antennas**	PLACE CP, vehicle, and manpack antennas behind **barriers**, **buildings**, **woods**, or **hills**.
8.	**REDUCE Power**	SHUT it OFF when not in **use**. SET radio to **low power**.
9.	**PRIORITIZE LPD Nets**	COMMUNICATE on **radio nets** that have LPD. KNOW which nets are more **vulnerable**.
10.	**PLAN Simple Flexible Ops**	PLAN operations that require **less radio calls.** PLAN **less nets**.

The United States Marine Corps (USMC) Publication Signature Management (SIGMAN) EP-EMCON-SOP - A Guide to Reduce Technical Signature, dated November 2020, lists ten ways for units in the field to reduce their electromagnetic emissions. These recommendations apply to large maneuver units as well as small squads and teams attempting to avoid detection by enemy signals intelligence (SIGINT) assets.

Isolated personnel should employ techniques to reduce electronic emissions whenever possible, thereby reducing the likelihood that they will be detected and targeted by hostile forces.

In addition to the techniques listed in SIGMAN, consider using directional antennas so that your signal is transmitted toward the intended receiving station with less signal radiating in other directions.

Frequency Hopping Spread Spectrum (FHSS) radios spread your signal over multiple frequencies, making it much more difficult to detect. Some FHSS radios are available from Motorola (such as the DTR700) and operate in the 900 MHz ISM Band. While these radios do have a true FHSS capability, they are expensive, and have limited range; but still might be of interest for team communications in the field.

Split communications, where you transmit on one frequency and receive on a different frequency (maybe in a different band) may prevent an adversary from hearing both sides of a conversation.

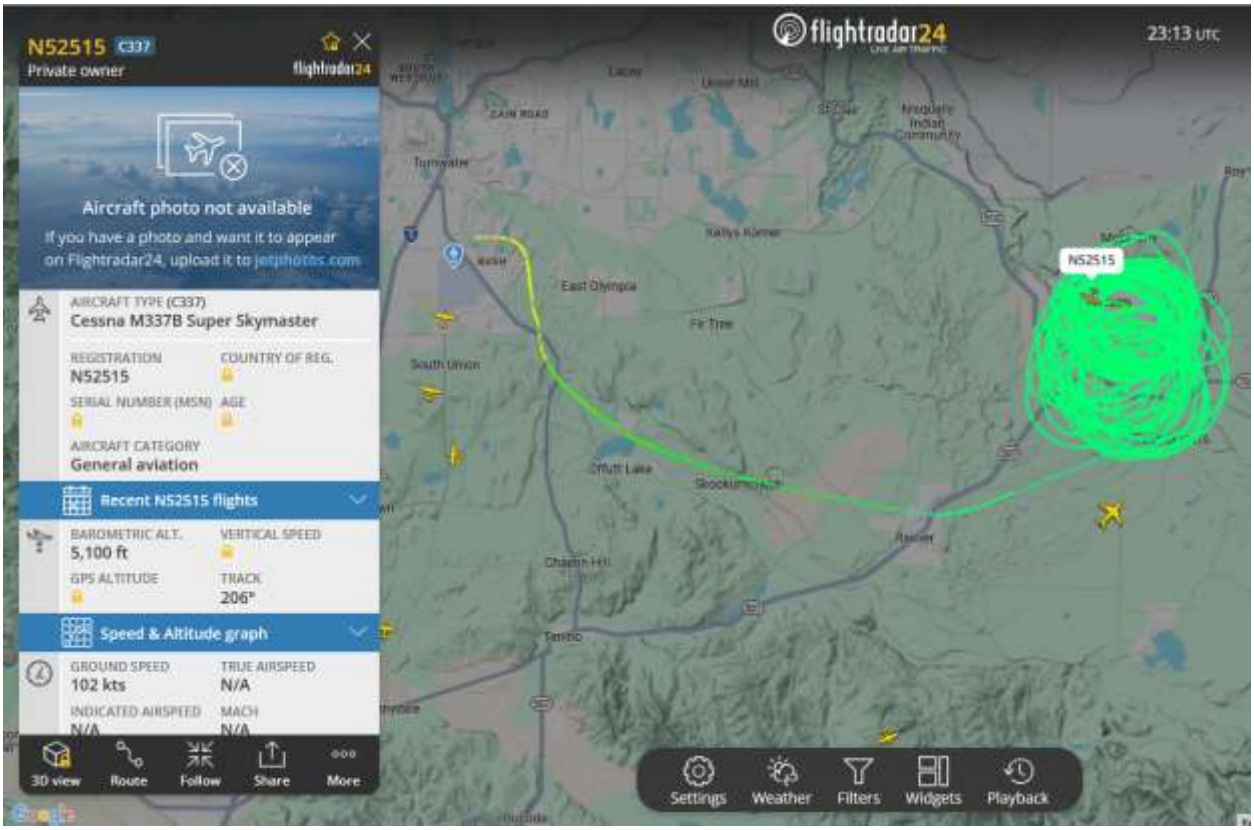
Ribbit (https://www.ribbitradio.org/#/) is a texting mode that encodes a message in what sounds like static or background noise and uses audio coupling to send and receive that message over HF/VHF/UHF analog radios. The Rattlegram app (available for both Android and iOS) allows you to use your cell-phone and a radio to send and receive text messages via radio. Play the audio into a radio on the transmitting end and record and decode the audio with the app on the receiving end.

All of these signature management techniques employ ‘security through obscurity’ – making your communications more secure by making them harder to detect, intercept, or locate.

But it is important to understand that adversaries may employ significant assets in an attempt to defeat that security and intercept your communications.

On April 22, 23, & 24, 2025 an aircraft owned and operated by a company with numerous government and military contracts flew a four-hour surveillance pattern each

day over the city of Yelm, WA. Yelm is located adjacent to the Joint Base Lewis-McChord military installation, and it seems likely that this flight was part of a military surveillance exercise to intercept electronic communications (cell-phone calls) and/or to conduct video and photographic surveillance of the local civilian community. The above figure shows the ADS-B track of the surveillance aircraft as recorded by FlightRadar24.



The Federal Bureau of Investigation (FBI) also maintains a fleet of covert aircraft that routinely conduct surveillance missions over U.S. cities. In a published statement on June 4, 2015, FBI Deputy Director Mark F. Giuliano stated" *"It should come as no surprise that the FBI uses planes to follow terrorists, spies, and serious criminals. We have an obligation to follow those people who want to hurt our country and its citizens, and we will continue to do so."*

While military and law enforcement surveillance of our communities may or may not be of concern to the average person living in an American city, the fact that this surveillance is occurring in the United States highlights the capabilities of government agencies to target isolated personnel in hostile and non-permissive environments.

"The enemy is focused on intercepting your radio signal [including cell-phone signals]. To do this, all the enemy needs is a radio receiver that operates in the same mode and on the same frequency you are using to transmit. The mere fact that you are operating gives the enemy valuable information. It tells the enemy that you are in the

area. By the number of stations operating on the same frequency, the enemy can estimate the size of the unit. If your net is operating in the clear, the enemy's language specialists can understand exactly what is said for even more information. When analyzing the traffic pattern, the enemy can figure out which station is the net control station (NCS) and identify the headquarters. Usually, in U.S. forces, the NCS is the radio used by the operations officer or section of the highest headquarters operating in the net. By further traffic analysis, the enemy can determine changes in the level of activity that could mean a movement or upcoming operation."

Radio Direction Finding – *"Interception is only one of the many dangers that the radio operator will face. After knowing friendly forces are in the area, the enemy will try to locate their position by using radio direction finding (RDF). A radio direction finder consists of a radio receiver, a directional antenna, and other specialized equipment. With RDF equipment, the approximate azimuth (i.e., bearing) to a transmitting radio can be determined. One azimuth gives a general indication of direction. The intersection of two azimuths by different RDF stations is called a cut and gives a general indication of distance. The intersection of three or more azimuths is called a fix and gives a general location. The ideal fix is the exact intersection of three or more bearings. However, exact intersection is seldom achieved.*

Terrain, weather, variations in radio wave propagation characteristics, the inherent RDF equipment, and operator inaccuracies, prevent an ideal fix. The fix that is obtained is called an actual fix. Although the actual fix may not be usable for immediate targeting purposes, it is more than enough for intelligence analysts to develop targeting data. Airborne direction finding is more accurate than ground-based direction finding but normally requires further analysis for targeting.

RDF ability to intercept electronics equipment emissions and determine a bearing depends on the power output of the targeting transmitter and its antenna radiation patterns. Experience indicates RDF accuracy of 500-meter (547-yard [yd]) circular error of probability (CEP) is considered a very good RDF fix. Normally, 50 percent of the CEPs are approximately 1,500 meters (1,640 yds) when the direction finder is located within 20 to 25 kilometers (12.4 to 15.5 mi) of the transmitter." (MCRP 6-22C, 7-10)

While the lost or stranded hiker in a national park may have little need for signature management when calling for help, if you are a hiker in Iraqi Kurdistan, near the Iranian border, signature management becomes critical – as we saw on July 31, 2009, when three Americans, Joshua Fattal, Sarah Shourd and Shane Bauer were taken into custody by Iranian border guards for crossing into Iran while hiking.

In January 2025 we saw two hikers, one U.S. citizen and one Canadian citizen, attacked by armed Mexican cartel terrorists, in the Jacumba Wilderness in San Diego

and Imperial Counties of California. The hikers were shot and robbed by the suspected terrorists, but were able to call 911 for assistance.

According to U.S. Customs and Border Patrol: *"At 12:08 p.m. Mountain Disrupt Unit, Border Patrol Tactical Unit (BORTAC), and Border Patrol Search Trauma, and Rescue (BORSTAR) agents infiltrated to the area, locating the injured victim and stabilizing him. Agents created a protective perimeter and extracted the victim via CBP Air and Marine Operations San Diego. The victim was transferred to Reach Air Ambulance and flown to Sharp Medical Center in San Diego for treatment. BORTAC and BORSTAR agents maintained a secure perimeter and tracked the assailants back to the border where they returned to Mexico."*

Whether you are hiking along the Iranian border, or hiking in a wilderness area in California (near the Mexican border) you may be targeted by a hostile force, requiring that you both evade detection by the enemy and communicate effectively with rescue forces that may be available to come to your aid. The need for secure communication and signature management isn't just a military requirement anymore.

Calling 911

911 is the North American Universal Emergency Number, allowing individuals requiring emergency assistance (Fire, Medical, Police) to dial one easily remembered number and be connected to a Public Safety Answering Point / dispatch center. Most countries have a similar three-digit emergency number, although the number may not be 911. For example, in the United Kingdom the number is 999 or 112, and in most of Europe and Russia the number is 112.

Call 911 only for actual emergencies. Examples of emergencies include a building on fire, serious injury or illness that prevents you from transporting yourself to the nearest hospital emergency room, or a serious crime in progress.

In 2018, Washington state DSHS published information on 'When to Call 911', stating in part…

Call 911 when:

- The condition is life or limb threatening
- The condition could worsen quickly on the way to the hospital
- Moving the victim will cause further injury
- The person needs skills, medication or equipment right away that paramedics carry
- Distance or traffic would delay transporting the person to the hospital and could be life threatening

Other situations when you should call 911

- Any crime in progress (robbery, burglary, prowler, fights, etc.)
- Any type of fire (structure, vehicle, brush, etc.)
- A vehicle collision, especially if someone is injured
- When you or the person you care for feels at risk.

Call 911 when you need an emergency response, but contact other services if all you need is assistance. There are only so many fire fighters, medics, and police officers in any given area. Call 911 when you need emergency services, but don't call 911 for non-emergency issues.

When calling 911 for an emergency response:

- Stay calm. Provide the 911 call-taker with:
- The location of the emergency. If you do not know the address, look for landmarks, street signs, or buildings. In a remote or wilderness area provide latitude / longitude (grid coordinates).
- The nature of the emergency (such as medical, fire, crime). Providing this information will help them determine which responder to send.
- Details about the emergency.
- Be ready to answer questions from the 911 call-taker.

All cell-phones, even those that are not subscribed to or supported by a specific carrier, can call 911. However, calls to 911 on phones without active service do not deliver the caller's location to the 911 call center, and the call center cannot call these phones back to find out the caller's location or the nature of the emergency. If disconnected, the 911 center has no way to call back the caller. (https://www.911.gov/)

While any cell-phone, regardless of whether it has a service plan or not, can place a call to 911, the phone must still be able to connect to the cellular network for this to work. In an area with no cellular coverage, your cell-phone will not be able to connect to 911 – service plan or not. If there is no available cellular network, there is no cellular connection to 911. Many areas still have limited or no cellular service. The more rural and remote an area is, the less likely it is that the area will have cellular coverage.

Cellular service providers build cell-towers and install cell-sites in locations to provide the best coverage of populated areas (places with paying customers). As you move into rural and remote areas, cell-towers become fewer and cellular service becomes less reliable. If you plan on relying on your cell-phone to call 911, confirm that you have a good cellular connection from your location.

Text to 911

In the United States, in addition to calling 911, you can Text 911 in many areas. In some states all Public Safety Answering Points are set up to receive texts to 911, while in other states, some rural areas may not have yet implemented the Text 911 service.

To send a text to 911, open your phone's text messaging program. Enter the numbers "911" in the "To" field (no quotation marks). Type a message with the exact location of the emergency and the type of emergency help needed (fire, medical, or police). Push the "Send" button. Stay with your phone, be prepared to answer questions and follow instructions from the 911 call taker.

Be aware of auto correct especially when providing a location. Do not send the same text message to multiple people at the same time. A "group text" may cause your message to 911 to fail. Do not use emoticons or other symbols and do not use abbreviations or acronyms (text speak). (https://mil.wa.gov/texting911)

Text to 911 routes your message to the nearest Public Safety Answering Point, based on where your message connected to the cellular network. However, especially in rural areas, your message may connect to the cellular network through a tower that is some distance away from your actual location.

"If you attempt to send a text to 911 where the service is not yet available, FCC rules require all wireless carriers and other text messaging providers to send an automatic "bounce-back" message that will advise you to contact emergency services by another means, such as making a voice call or using telecommunications relay service. Bounce-back messages are intended to minimize your risk of mistakenly believing that a text to 911 has been transmitted to an emergency call center when it has not." (https://www.fcc.gov/consumers/guides/what-you-need-know-about-text-911)

Text to 911 requires a text or data plan to work. While a voice call to 911 will go through on a cell-phone that is not subscribed, a text to 911 requires that the phone be subscribed and supported by a cellular service provider (i.e. AT&T, T-Mobile, Verizon).

If, however, you have poor cellular service and find that you can't get a voice call to connect to 911, it may be that a text to 911 will still go through. SMS messaging does not require a data connection to function. Unlike messaging apps like WhatsApp or Facebook Messenger, which rely on an internet connection to send messages, SMS operates on a separate channel. This means that you can send and receive text messages even when you have no Wi-Fi or cellular data available. While SMS does not require a Wi-Fi connection to function, having Wi-Fi enabled on your device can still be beneficial. Some smartphones have the capability to send SMS messages over Wi-Fi when the cellular network is weak or unavailable. This feature can help ensure that your messages are delivered promptly, even in areas with poor network coverage.

Military Manuals and Communications References

Most military manuals are focused on TTPs that are specific to military operations, however in the case of radio operations, military and amateur radio overlap. Radio theory is the same, regardless of who is running the radio. The following military manuals provide useful information for amateur radio operators.

- Antenna Handbook - MCRP 8-10B.11 - USMC (2 May 2016)
- Auxiliary Communications Field Operations Guide (AUXFOG) (June 2016)
- Communications-Electronics Fundamentals - Wave Propagation Transmission Lines and Antennas - TC 9-64 (July 2004)
- High Frequency Radio Communications - US Army FM 11-65 (October 1978)
- National Interoperability Field Operations Guide (NIFOG) (January 2025)
- Radio Operators Handbook - MCRP 3-40.3B - USMC (1999)
- Reconnaissance Reports Guide - MCRP 2-10A.7 (12 April 1998)
- Secure Communications with the One-Time Pad Cipher -by Dirk Rijmenants (27 February 2022)
- Signature Management (SIGMAN) EP-EMCON-SOP - A Guide to Reduce Technical Signature (1 November 2020)
- Survival Evasion Resistance Escape (SERE) Operations (AF Handbook 10-644) (27 March 2017)
- Tactical Radio Operations - FM 6-02-53 (2020)
- US Special Forces Radio Antennas (1974)
- Visual Signals TC 3-21.60 (March 2017)

NATO phonetic alphabet, codes & signals

The ability to communicate and make yourself understood can make a difference in life-threatening situations – imagine for example that you are trying to alert a search and rescue helicopter of the position of a downed pilot. To ensure clear communication, NATO uses a number of well-known formats which are in general use. NATO standardization agreements enable forces from many nations to communicate in a way that is understood by all.

Some standards can be found in everyday civilian and military life. "Bravo Zulu", typically signalled with naval flags on ships at sea and meaning "well done", is also commonly used in written communication by the military, for example by replying "BZ" to an email.

Phonetic alphabet

The NATO alphabet became effective in 1956 and, a few years later, turned into the established universal phonetic alphabet for all military, civilian and amateur radio communications.

International Morse Code

Morse code transmits text through on-off tones, light flashes or clicks. It was widely used in the 1990s for early radio communication, before it was possible to transmit voice.

Flaghoist communication

Ships use flags as signals to send out messages to each other. The use of flags, known as flaghoist communication, is a fast and accurate way to send information in daylight.

Semaphore

Semaphore is a system in which a person sends information at a distance using hand-held flags – depending on the position of the flags, the message will vary. The signaller holds the flag in different positions that represent letters or numbers.

Panel signalling

Panels are visual signals for sending simple messages to an aircraft. Using a limited code, ground forces can send messages to pilots, for example to request medical supplies.

Numbers